Die Beauftragte
der Bundesregierung
für Informationstechnik

# Migrationsleitfaden

## Leitfaden für die Migration von Software

**Version 4.0**

**November 2011**

# Vorwort zur vierten Version des Migrationsleitfadens

Der Migrationsleitfaden bietet IT-Entscheidern einen Überblick über alle wichtigen Aspekte von Softwaremigrationen sowie eine praktische Hilfe für deren Planung und Durchführung. In der vorliegenden Version 4 wurde der Migrationsleitfaden vollständig überarbeitet und einige bisher enthaltene Bestandteile als eigenständige Dokumente ausgelagert. Die bisherige Beschreibung einzelner Migrationspfade wurde wegen der stark heterogenen Ursprungs- und Zielsysteme einzelner Behörden sowie der schnellen Alterung betrachteter Software-Versionen aufgegeben. Stattdessen finden sich nun Entscheidungshilfen für die jeweiligen Migrationsgebiete in Form von Kriterienlisten, kurzen Produktbeschreibungen, tabellarischen Gegenüberstellungen und Empfehlungen.

Die (Bundes-)Verwaltung ist seit langem selbst oder als Auftraggeberin im Bereich der Softwareentwicklung tätig. Dabei hat der Anteil an verwendeten oder veränderten Open-Source-Komponenten in den letzten Jahren stetig zugenommen. Die Verwaltung ist insbesondere durch den Rückfluss von Änderungen und Erweiterungen an die jeweilige Produkt-Community in einigen Fällen implizit ein Teil der Open-Source-Community geworden. Die hierbei aufgekommenen rechtlichen Fragen werden im Migrationsleitfaden aufgegriffen. Die Betrachtung der rechtlichen Aspekte von Softwaremigrationen wurde vollständig überarbeitet und aktualisiert. Deren Kernaussagen sind im Migrationsleitfaden enthalten und schlagen die Brücke zur Gesamtbetrachtung rechtlicher Aspekte von Softwaremigrationen, die dem Migrationsleitfaden als eigenständiges Dokument zur Seite gestellt ist. Neu darin sind die Abschnitte über die Lizenzierung verwaltungseigener Software als Open-Source-Software und über die Modifizierung von Open-Source-Software durch die Verwaltung.

Die Wirtschaftlichkeitsbetrachtung von Software-Migrationen wurde analog zu den rechtlichen Aspekten behandelt. Deren Kernaussagen sind weiterhin im Migrationsleitfaden enthalten und verweisen für die Details auf das entsprechende Begleitdokument.

# Inhaltsverzeichnis


**Vorwort zur vierten Version des Migrationsleitfadens** . . . . . III

**1 Einleitung** . . . . . 1
- 1.1 Ziele des Dokuments . . . . . 1
- 1.2 Zielgruppe . . . . . 2
- 1.3 Aufbau und Inhalt . . . . . 2

**2 Begriffe** . . . . . 5
- 2.1 Migration . . . . . 6
  - 2.1.1 Aktualisierung . . . . . 6
  - 2.1.2 Fortführende Migration . . . . . 6
  - 2.1.3 Ablösende Migration . . . . . 7
  - 2.1.4 Migrationswege . . . . . 7
- 2.2 Offene Standards . . . . . 9
- 2.3 Konformität und Interoperabilität . . . . . 11
- 2.4 Schnittstellen, Module, Komponenten und Services . . . . . 12
- 2.5 Integration . . . . . 13
  - 2.5.1 Integrationsformen . . . . . 13
    - 2.5.1.1 Zusammenstellungen . . . . . 13
    - 2.5.1.2 Funktionale Integration . . . . . 13
    - 2.5.1.3 Datenintegration . . . . . 13
    - 2.5.1.4 Kombinierte Integration . . . . . 14
  - 2.5.2 Integrationshilfen . . . . . 14
  - 2.5.3 Integration und Standardisierung . . . . . 14
  - 2.5.4 Integration und Abhängigkeit . . . . . 14
  - 2.5.5 Fazit . . . . . 16
- 2.6 Open-Source-Software . . . . . 17
  - 2.6.1 Standardisierung und Open-Source-Software . . . . . 17
  - 2.6.2 Open-Core-Software . . . . . 17
  - 2.6.3 Produkteinsatz . . . . . 18
  - 2.6.4 Entstehung von OSS . . . . . 19
- 2.7 Proprietäre Software . . . . . 20
  - 2.7.1 Freeware . . . . . 20
  - 2.7.2 Shareware . . . . . 20

**3 Kriterien für erfolgreiche Migrationen** . . . . . 21
- 3.1 Ziele einer Migration . . . . . 21
- 3.2 Vorgehensweise / Migrationsplanung . . . . . 22

3.2.1 Einführungsphase . . . 23
3.2.2 Anforderungsanalysephase . . . 24
3.2.3 Auswahlphase . . . 25
3.2.4 Umsetzung . . . 25
3.2.4.1 Stichtagsumstellung . . . 25
3.2.4.2 Schrittweise Migration . . . 26
3.2.5 Kompetenzzentrum Open-Source-Software . . . 27
3.3 Strategische Aspekte . . . 28
3.4 Rechtliche Aspekte . . . 29
3.4.1 Behörde als Nutzer und Lizenznehmer . . . 29
3.4.2 Lizenzierung verwaltungseigener Software als OSS . . . 30
3.5 Wirtschaftliche Aspekte . . . 33
3.6 Qualitative Aspekte . . . 34
3.6.1 Funktionale Eignung . . . 34
3.6.2 Leistungsfähigkeit . . . 34
3.6.3 Kompatibilität . . . 34
3.6.4 Benutzbarkeit . . . 35
3.6.5 Zuverlässigkeit . . . 35
3.6.6 Sicherheit . . . 35
3.6.7 Wartbarkeit . . . 35
3.6.8 Portabilität . . . 36
3.6.9 Dokumentationsgüte . . . 36
3.6.10 Konfigurierbarkeit . . . 36
3.6.11 Sonstige Qualitätsmerkmale . . . 37
3.7 Aspekte des Systembetriebs . . . 38
3.7.1 Weitere Arten der Migration aus Sicht des Systembetriebs . . . 38
3.7.2 Service Level Agreements (SLAs) . . . 38
3.7.3 Anforderung an das Migrationsvorgehen . . . 39
3.7.4 Auswahl der Infrastruktur und der Anwendungsprodukte . . . 39
3.7.5 Wartungsverträge und Lizenzmodelle . . . 40
3.7.6 Auswahl des Systembetreibers . . . 40
3.8 Organisatorische Aspekte . . . 42
3.8.1 Change Management . . . 42
3.8.2 Release Management . . . 43
3.8.3 Zeitplanung . . . 43
3.8.4 Risikomanagement . . . 44
3.8.5 Veränderungsmanagement innerhalb der IT . . . 44
3.8.6 Veränderungsmanagement innerhalb der Anwenderorganisation . . . 45
3.8.7 Einführungs- und Schulungskonzept . . . 46
3.8.8 Stakeholder . . . 46
3.8.9 Management-Unterstützung . . . 47
3.9 Sicherheitsaspekte . . . 48
3.9.1 Informationssicherheit . . . 48
3.9.2 Schutzziele der Informationssicherheit . . . 48
3.9.3 Strukturanalyse nach IT-Grundschutz . . . 49
3.9.4 Bewertungskriterien . . . 49
3.9.4.1 Sicherheitskriterien zur Anforderungsanalyse . . . 49
3.9.4.2 Sicherheitskriterien zum Migrationsprojekt . . . 50

3.9.4.3 Umsetzungsbewertung der Anforderungskriterien . . . 51
3.10 Exkurs: Erfahrungsbericht der Landeshaupstadt München – Projekt LiMux . . . 52
3.10.1 Historie und Ziele des Projekts LiMux . . . 52
3.10.2 Projektinhalt/Projektgegenstand . . . 52
3.10.2.1 Heterogenität der Clients . . . 53
3.10.2.2 Zwei verschiedene Fileservice-Systeme . . . 53
3.10.2.3 Zentrale Strategie und dezentraler Berieb . . . 53
3.10.2.4 Bestandteile des linuxbasierten PC Arbeitsplatzes . . . 53
3.10.3 Projektsteuerung . . . 53
3.10.4 Projektorganisation . . . 54
3.10.5 Projektmethodik . . . 54
3.10.6 Projektvorgehen . . . 54

**4 Migrationsgebiete . . . 57**
4.1 Übersicht . . . 57
4.1.1 Aufbau . . . 58
4.1.2 Bewertungs-Skalen . . . 58
4.1.3 Bewertungsmethode . . . 59
4.1.4 Domänen-Spezifika . . . 59
4.2 Infrastruktur . . . 60
4.2.1 Low-Level-Dienste . . . 60
4.2.1.1 Adress-Vergabe und Netzwerkkonfiguration . . . 60
4.2.1.2 Namensauflösung . . . 61
4.2.1.3 Dateiablage . . . 61
4.2.1.4 Druckdienste . . . 61
4.2.1.5 Komplettlösungen und Distributionen . . . 62
4.2.2 System-Überwachung . . . 64
4.2.2.1 Einleitung . . . 64
4.2.2.2 Kriterienkatalog . . . 65
4.2.2.3 Methodik . . . 66
4.2.2.4 Betrachtete Alternativen . . . 66
4.2.2.5 Bewertung . . . 66
4.2.2.6 Empfehlungen . . . 69
4.2.2.7 Ausblick . . . 70
4.2.3 Authentisierungs- und Verzeichnisdienste . . . 71
4.2.3.1 Einleitung . . . 71
4.2.3.2 Kriterienkatalog . . . 71
4.2.3.3 Methodik . . . 72
4.2.3.4 Betrachtete Alternativen . . . 72
4.2.3.5 Bewertung . . . 72
4.2.3.6 Empfehlungen . . . 75
4.2.3.7 Migrations-Checkliste . . . 75
4.2.4 Groupware . . . 77
4.2.4.1 Einleitung . . . 77
4.2.4.2 Kriterienkatalog . . . 77
4.2.4.3 Methodik . . . 78
4.2.4.4 Betrachtete Alternativen . . . 78
4.2.4.5 Bewertung . . . 78

4.2.4.6 Bewertungstabelle . . . 82
4.2.4.7 Empfehlungen . . . 82
4.2.4.8 Migrations-Checkliste . . . 83
4.2.5 Virtualisierung und Terminaldienste . . . 85
4.2.5.1 Einleitung . . . 85
4.2.5.2 Kriterien . . . 88
4.2.5.3 Ist-Analyse . . . 89
4.2.5.4 Soll-Konzeption . . . 89
4.2.5.5 Produktauswahl . . . 91
4.2.5.6 Bewertung . . . 92
4.2.5.7 Empfehlungen . . . 103
4.2.5.8 Terminaldienste . . . 103
4.2.6 Client-Management . . . 105
4.2.6.1 Einleitung . . . 105
4.2.6.2 Kriterienkatalog . . . 105
4.2.6.3 Methodik . . . 106
4.2.6.4 Betrachtete Alternativen . . . 106
4.2.6.5 Empfehlungen . . . 109
4.3 Desktop und unterstützende Systeme . . . 111
4.3.1 Einleitung . . . 111
4.3.2 Web-Browser . . . 112
4.3.2.1 Einleitung . . . 112
4.3.2.2 Kriterienkatalog . . . 112
4.3.2.3 Methodik . . . 112
4.3.2.4 Betrachtete Alternativen . . . 115
4.3.2.5 Bewertung . . . 115
4.3.2.6 Bewertungstabelle . . . 118
4.3.2.7 Empfehlungen . . . 119
4.3.2.8 Migrations-Checkliste . . . 119
4.3.3 Personal Information Manager . . . 121
4.3.3.1 Einleitung . . . 121
4.3.3.2 Kriterienkatalog . . . 121
4.3.3.3 Methodik . . . 121
4.3.3.4 Betrachtete Alternativen . . . 122
4.3.3.5 Bewertung . . . 122
4.3.3.6 Bewertungstabelle . . . 126
4.3.3.7 Empfehlungen . . . 127
4.3.3.8 Migrations-Checkliste . . . 127
4.3.4 Office-Suiten . . . 129
4.3.4.1 Einleitung . . . 129
4.3.4.2 Ist-Analyse . . . 129
4.3.4.3 Soll-Konzeption . . . 132
4.3.4.4 Betrachtete Alternativen . . . 134
4.3.4.5 Bewertung . . . 134
4.3.4.6 Empfehlungen . . . 145
4.3.4.7 Migrations-Checkliste . . . 146
4.3.5 Dokumenten Management Systeme . . . 149
4.3.5.1 Einleitung . . . 149

4.3.5.2 Kriterienkatalog . . . 149
4.3.5.3 Methodik . . . 151
4.3.6 Web Content Management Systeme . . . 155
4.3.6.1 Einleitung . . . 155
4.3.6.2 Kriterienkatalog . . . 155
4.3.6.3 Methodik . . . 158
4.3.6.4 Aktuell relevante Alternativen . . . 160
4.3.6.5 Migrations-Checkliste . . . 160
4.3.7 PDF-Reader und -Authoring . . . 163
4.3.7.1 Einleitung . . . 163
4.3.7.2 Kriterienkatalog . . . 163
4.3.7.3 Methodik . . . 164
4.3.7.4 Betrachtete Alternativen . . . 165
4.3.7.5 Bewertung . . . 165
4.3.7.6 Empfehlungen . . . 169

**5 Zukunftsthemen der IT . . . 171**
5.1 Cloud Computing . . . 171
5.2 Infrastruktur und Desktop-Anwendungen in der Cloud . . . 172
5.3 Neue IT-Infrastruktur-Elemente . . . 172

# Kapitel 1

# Einleitung

Behörden entwickeln ihre IT-Systemlandschaften stetig weiter. Die Gründe dafür sind vielfältig, beispielsweise auslaufende Hersteller-Unterstützung für bestimmte Produkte, erweiterte technische oder fachliche Anforderungen, die Konsolidierung der Systemlandschaften oder die Umsetzung strategischer Ziele.

Solche Weiterentwicklungen sind stets mit Änderungen an der bestehenden Systemlandschaft verbunden. Beispiele sind

- die Ablösung einzelner Komponenten durch stark weiterentwickelte oder alternative Varianten,
- die Erweiterung um neue Komponenten und deren Integration in bestehende Teilsysteme oder
- die Ablösung eines Betriebssystems durch ein anderes samt der Anpassung der darauf laufenden Anwendungen und Daten.

In jedem Fall wird das Gesamtsystem in einen deutlich veränderten Zustand versetzt. Es handelt sich damit um eine Software-Migration (von lateinisch *migratio* für „Wanderung“ oder „Übersiedlung“).

Eine Software-Migration ist ein vielschichtiger Prozess, der die Verantwortlichen fordert. Es müssen rechtliche Aspekte gewürdigt, die Wirtschaftlichkeit betrachtet und verbindliche strategische Entscheidungen übergeordneter Instanzen eingehalten werden. Die einzelnen Migrationsgebiete müssen vor dem Hintergrund der behördenweiten Gesamtsystemarchitektur beleuchtet und das jeweilige Optimum ermittelt werden. Und nicht zuletzt gilt es, die Auswirkungen von Änderungen an bestehenden Systemlandschaften auf den IT-Betrieb, die Systemsicherheit und die Anwender zu berücksichtigen.

## 1.1 Ziele des Dokuments

Der Migrationsleitfaden begleitet diese Schritte und hilft bei der Verbesserung des jeweiligen Migrationsprozesses. Er verschafft dem Leser[1] einen Überblick über die wesentlichen Aspekte von Migrationen, zeigt ihm die notwendigen Handlungsfelder auf und beantwortet die wichtigsten Fragestellungen. Auf dem Weg zu einem schlüssigen Gesamtkonzept versorgt er ihn bei der Entscheidung in den einzelnen Migrationsgebieten durch bewertete Alternativen und ausgesprochene Empfehlungen mit Argumenten für eine konkrete Migration.

Ergänzend zu den bisher genannten Zielen trägt der Migrationsleitfaden auch dazu bei, die heterogenen Systemlandschaften der Bundesbehörden zu konsolidieren und das entsprechend breit gestreute

[1] Aus Gründen der besseren Übersichtlichkeit und Lesbarkeit wird hier und im Folgenden auf die Verwendung von Paarformen verzichtet. Stattdessen wird die grammatisch maskuline Form verallgemeinernd verwendet. Diese Bezeichnungsform umfasst gleichermaßen weibliche und männliche Personen, die damit selbstverständlich gleichberechtigt angesprochen sind.

Wissen der IT-Fachkräfte auf die wesentlichen Themengebiete zu konzentrieren. Diese Wissenskonzentration hilft zudem bei der Personalgewinnung, da die Anforderungsprofile dadurch geschärft und auf konkrete Standards fokussiert werden können.

Alle beleuchteten Aspekte, Bewertungen und Empfehlungen verstehen sich als Hilfen zur Umsetzung des Konzepts IT-Steuerung Bund und der darauf basierenden Beschlüsse des Rats der IT-Beauftragten der Ressorts (IT-Rat)

- zur Rahmenarchitektur IT-Steuerung Bund[2],
- zur Einführung offener Dokumentenformate in der Bundesverwaltung[3],
- zum Konzept für SAGA 5[4] und
- zur IT-Konsolidierung in den zentralen IT-Dienstleistungszentren des Bundes (DLZ-IT).

## 1.2 Zielgruppe

Der Migrationsleitfaden richtet sich primär an Bedienstete des Bundes, die kraft ihres Amtes für die Pflege und Weiterentwicklung bestehender IT-Systeme oder für die Konzeption und/oder Realisierung neuer IT-Systeme verantwortlich sind (IT-Entscheider) oder die Projekte leiten, in deren Rahmen Migrationen zu berücksichtigen oder umzusetzen sind.

Personen, die auf Grund eines politischen Mandats in diese Themen involviert sind, können sich aus dem Migrationsleitfaden mit Hintergrundwissen versorgen. Zuarbeiter von IT-Entscheidern, die beispielsweise mit der Erstellung einer Wirtschaftlichkeitsbetrachtung für eine Migration beauftragt sind, finden im Migrationsleitfaden detaillierte Bewertungshilfen.

Systemadministratoren und Anwender der Software-Systeme gehören nicht zur Zielgruppe des Migrationsleitfadens, sind aber gleichwohl zu dessen Lektüre eingeladen, um Entscheidungen nachzuvollziehen oder sich auf kommende Migrationen vorzubereiten. Auch alle sonstigen Bediensteten der öffentlichen Verwaltungen können die für sie relevanten Themen mit den Inhalten des Migrationsleitfadens abgleichen und sich daraus ggf. für den eigenen Bereich mit Anregungen oder Argumenten versorgen.

## 1.3 Aufbau und Inhalt

Der Aufbau des Migrationsleitfadens orientiert sich an der in vielen Projekten bewährten Herangehensweise von IT-Entscheidern bei der Betrachtung von Migrationsvorhaben. Indem zunächst die grundsätzlichen Aspekte beleuchtet und Rahmenbedingungen für die konkrete Migration abgesteckt werden, ist der Blick anschließend frei für das eigentliche Vorhaben und die Bewertung der Alternativen innerhalb des gesteckten Rahmens.

Der Migrationsleitfaden führt im Kapitel 2 die wichtigsten Begriffe im Umfeld von Migrationen ein. Die verschiedenen Migrations- und Integrationsarten sowie die Abhängigkeitsgrade werden erläutert, quelloffene und proprietäre Software voneinander abgegrenzt und die Prinzipien der Modularisierung vorgestellt.

Das Kapitel 3 behandelt die übergreifenden Kriterien für den Erfolg von Migrationen. Nach den Zielen und der Vorgehensweise werden die verschiedenen Aspekte einer Migration und deren grundsätzliche Bewertung betrachtet. In diesem Kapitel wird außerdem auf die begleitenden Dokumente zu rechtlichen Aspekten und der Wirtschaftlichkeitsbetrachtung von Software-Migrationen hingewiesen und deren wichtigste Aussagen in Kurzform wiedergegeben.

[2] http://www.rahmenarchitektur.de
[3] http://www.cio.bund.de/odf
[4] http://www.cio.bund.de/saga

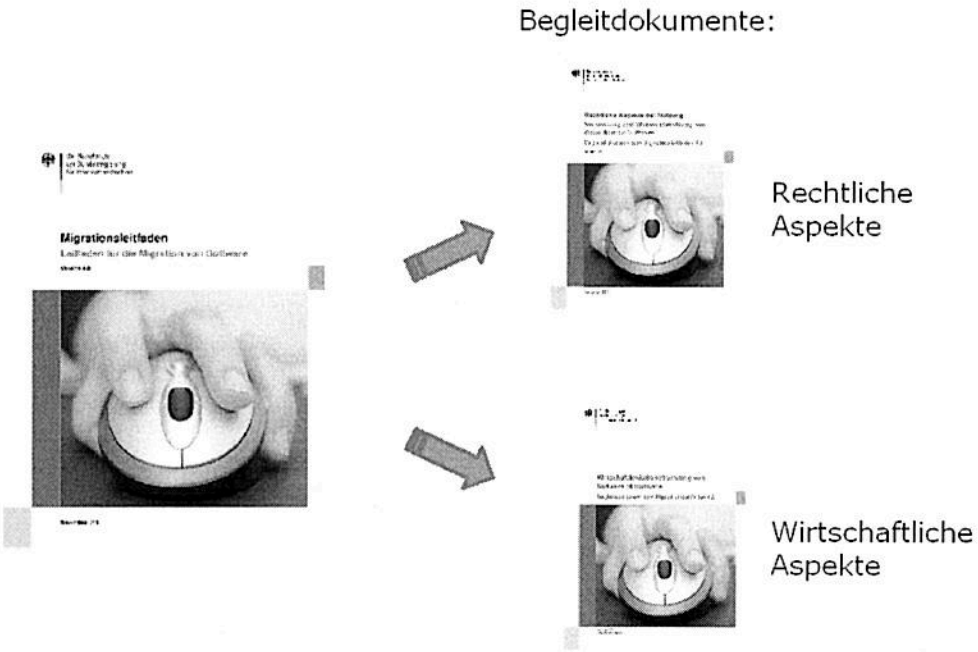


**Abbildung 1.1:** Die Begleitdokumente des Migrationsleitfadens

In Kapitel 4 werden die einzelnen Migrationsgebiete betrachtet, unterschieden nach Infrastruktur, Desktop und unterstützende Systeme. Das Kapitel 5 beschließt den Migrationsleitfaden mit Zukunftsthemen der IT.

# Kapitel 2

# Begriffe

Jede Migration von IT-Systemen ist anders. Unterschiede betreffen beispielsweise das Vorgehen ebenso wie den vorhandenen Grad an Abhängigkeit der betroffenen Komponenten, deren aktuellen oder künftigen Integrationsgrad ebenso wie den Einsatz quelloffener oder proprietärer Produkte. Bei größeren Systemen spielt der vorhandene und der gewünschte Grad an Modularisierung eine wichtige Rolle, und auch die Behördengröße und das vorhandene IT-Personal sind wesentliche Rahmenbedingungen von Software-Migrationen.

Es ist daher nicht praktikabel, Migrationen stets aus derselben Blickrichtung zu betrachten. Vielmehr gilt es, die Charakteristika einer konkreten Migration zu erfassen, um sie in die im nächsten Kapitel vorgestellten übergreifenden Kriterien einfließen lassen zu können. Erst wenn klar ist, um was für eine Migration es sich im jeweiligen Bezug handelt, kann eine belastbare Entscheidung getroffen werden.

Die Begriffe zur Erfassung dieser Charakteristika werden nachfolgend vorgestellt und im weiteren Verlauf des Migrationsleitfadens an verschiedenen Stellen verwendet. Zunächst werden die für den Migrationsleitfaden elementaren Begriffe „Migration“ und „Offene Standards“ eingeführt und die dafür anzulegenden Kriterien erläutert. „Konformität und Interoperabilität“ befasst sich mit der Bewertung der Einhaltung von Standards. An welchen Stellen Standards in Software-Architekturen wichtig sind, wird unter „Schnittstellen, Module, Komponenten und Dienste“ beleuchtet. Die verschiedenen Grade von Integration und deren Auswirkungen auf Software-Systeme werden im gleichnamigen Unterkapitel dargestellt. Unter „Open-Source-Software“ und „Proprietäre Software“ werden schließlich die lizenzrechtlichen Gegenpole der Software-Bereitstellung voneinander abgegrenzt

## 2.1 Migration

Eine Migration ist eine wesentliche Veränderung der vorhandenen Systemlandschaft oder eines beträchtlichen Teils derselben. Veränderungen der Systemlandschaft treten allerdings vielfach auf, und nicht jede Änderung ist wesentlich.

Nahezu jedes Software-Produkt verfolgt seine eigene Versionierungs-Philosophie. Oftmals spielen Marketingaspekte hinein, um beispielsweise formal mit dem Versionsstand eines Konkurrenzprodukts gleichzuziehen. Die Unterschiede in den Bezeichnern der zu vergleichenden Versionen eines Produkts bieten daher regelmäßig keinen verlässlichen Anhaltspunkt für den Grad an Änderungen.

Es ist daher zu klären, wo Änderungen auftreten können und welche Auswirkungen sie auf die Systemlandschaft haben, um auf dieser Basis eine begriffliche Abgrenzung zu erreichen.

### 2.1.1 Aktualisierung

Unter einer Aktualisierung (engl. Update) wird die einfache Erneuerung eines bestehenden Produktes verstanden. Sie weist folgende Eigenschaften auf:

1. Die Produktlinie wird nicht verlassen.
2. Die Einbettung der aktuellen Version in die bisherige Systemumgebung gelingt wegen der Abwärtskompatibilität problemlos, da Funktionalität nicht abgeschaltet, sondern ggf. als „deprecated“ (hinfällig) gekennzeichnet wird.
3. Die Aktualisierung ist regelmäßig ohne die Hilfe eigens dafür geschulten Personals möglich.
4. Anwender und Administratoren müssen für die Verwendung der aktualisierten Version nicht erneut geschult werden.
5. Es ist keine Ausschreibung für neue Software-Lizenzen durchzuführen.
6. Es ist keine Neu- oder Ersatzbeschaffung von Geräten aufgrund der Aktualisierung notwendig.

Aktualisierungen sind nicht Gegenstand der Betrachtungen des Migrationsleitfadens.

### 2.1.2 Fortführende Migration

Eine fortführende Migration (engl. Upgrade) ist eine komplexe Form der Erneuerung eines Produkts mit folgenden Eigenschaften:

1. Die Produktlinie wird nicht verlassen.
2. Die neue Produktversion beinhaltet grundlegende Änderungen, die wesentliche Auswirkungen auf das Produkt selbst oder dessen Kompatibilität mit dem bisherigen Umfeld haben.
3. Die Kriterien Nr. 3 bis 6 aus 2.1.1 Aktualisierung treffen zumindest teilweise nicht mehr zu.
4. Vorhandene Datenbestände können ohne oder mit wenig Transformationsaufwand übernommen werden.
5. Der Produkthersteller stellt ausreichende Hilfsmittel wie Migrationsassistenten, entsprechende Dokumentation oder einen dafür geschulten Service Desk zur Verfügung, um den Versionswechsel ohne sonstige externe Unterstützung bewältigen zu können.

Zur Prüfung dieser Eigenschaften sollten entsprechende Informationen vom Hersteller eingeholt, Releasenotes zu den zwischenzeitlichen Produktversionen studiert und diesbezügliche Veröffentlichungen Dritter beachtet werden. Außerdem sollten bereitgestellte Werkzeuge für den Versionswechsel geprüft und ein testweiser Versionswechsel samt einem Testverfahren zur Überprüfung der Kompatibilität durchgeführt werden.

Die häufigste Form der fortführenden Migration ist das Ersetzen des derzeit eingesetzten Produkts durch dessen nächste Version innerhalb derselben Generation[1]. Sind die zwischenzeitlich bereitgestellten Fehlerbereinigungen, Service Packs und sonstigen Aktualisierungen eingespielt worden, ist der Erfolg einer solchen fortführenden Migration wahrscheinlich.

Das Überspringen zwischenzeitlich erschienener Produktgenerationen hingegen ist mit deutlichem Mehraufwand verbunden. Bereitgestellte Änderungsdokumente und Migrationswerkzeuge der Hersteller sind für den Wechsel zur unmittelbar folgenden Generation konzipiert. Analoges gilt für einen ggf. vorhandenen Service Desk. Somit müssen für jeden Generationswechsel die dafür vorgesehenen Unterlagen studiert und die dafür bereitgestellten Werkzeuge eingesetzt werden. Zwischenzeitliche Aktualisierungen der übersprungenen Produktgeneration(en) müssen nachgezogen werden, so dass eine solche Gesamtmigration aus vielen Schritten besteht. Da Abweichungen in der vorgesehenen Aktualisierungs-Reihenfolge wie das Übersehen eines Schrittes oder ein zum falschen Zeitpunkt eingespielter Patch zu gravierenden Fehlern führen können, bietet eine derart umfangreiche Migration keine Gewähr für ein stabiles Produkt in der gewünschten Aktualität.

Aus diesen Gründen ist eine komplexe Erneuerung über mehrere Produktgenerationen hinweg nicht mehr als fortführende, sondern als ablösende Migration zu betrachten.

### 2.1.3 Ablösende Migration

Die ablösende Migration ist die gravierendste Form einer Systemänderung und weist mindestens eine der folgenden Eigenschaften auf:

1. Die Produktlinie wird verlassen oder mindestens eine Produktgeneration übersprungen.
2. Datenstruktur/-haltung, Benutzer-/Binärschnittstellen oder die Gesamtfunktionalität ändern sich wesentlich und es besteht keine Abwärtskompatibilität.
3. Es stehen weder geeignete Migrationswerkzeuge noch entsprechende Dokumentation zur Verfügung.
4. Eine längerfristige Hinzuziehung externer Experten ist notwendig.

Eine ablösende Migration bedarf einer gründlichen Analyse der zu erwartenden Änderungen, des daraus resultierenden Anpassungsbedarfs im Gesamtsystem, der aktuellen und künftigen Herstellerabhängigkeiten, der betrieblichen und organisatorischen Auswirkungen sowie vorbereitender und begleitender Maßnahmen zur Unterstützung der Anwender und Administratoren.

Darüber hinaus sind bei einer ablösenden Migration verstärkt strategische Vorgaben wie die Verwendung offener Standards zu beachten, die rechtlichen und wirtschaftlichen Aspekte zu beleuchten, die übrigen in Kapitel 3 genannten Kriterien abzuwägen und künftige Entwicklungen einzuschätzen.

### 2.1.4 Migrationswege

Es lassen sich zwei unterschiedliche Wege bei einem Migrationsvorhaben beschreiten: die Stichtagsumstellung und die schrittweise Migration.

[1] Eine Produktgeneration umfasst verschiedene Versionen eines Produkts mit zeitlicher und funktionaler Nähe ohne grundlegende Änderungen bei Datenhaltung, Benutzersteuerung, Schnittstellen und Abläufen.

Die Stichtagsumstellung ist durch einen kurzen Umstellungszeitraum geprägt, dessen Beginn und Ende mit geringem Abstand terminiert sind und idealerweise auf denselben Tag fallen. Das Ziel ist ein abrupter Wechsel des (Teil-)Systems, durch den der parallele Betrieb von Alt- und Neusystemen vermieden werden soll.

Die schrittweise Migration basiert auf dem Prinzip der Aufteilung komplexer Zusammenhänge in einzelne beherrschbare Aufgaben, die das Risiko des Gesamtvorhabens auf ein jeweils überschaubares Maß reduzieren sollen. Eine schrittweise Migration weist einen längeren Umstellungszeitraum auf, der bei komplexeren Vorhaben zudem in Phasen unterteilt wird, die mehrere Schritte zusammenfassen. Jeder Schritt umfasst dabei die Umstellung einer oder weniger voneinander abhängiger Komponenten als funktionaler Einheit. Bei einer großen Anwenderzahl kann eine funktionale Einheit in mehreren Schritten mit je einem Teil der umzustellenden Arbeitsplätze migriert werden. Analog zur Stichtagsumstellung werden auch beim schrittweisen Vorgehen Beginn und Ende der jeweiligen Migrationsschritte terminiert, woraus sich die Daten der einzelnen Phasen und der Gesamtmigration herleiten lassen.

Die Vor- und Nachteile beider Migrationswege werden im Rahmen der Vorgehensweise und der Migrationsplanung in Unterkapitel 3.2 diskutiert. Ein aktiv betriebenes IT- oder übergreifendes Architekturmanagement kann hier helfen, eventuell vorhandene Auswirkungen auf die Gesamt-IT-Landschaft abzuschätzen.

## 2.2 Offene Standards

Der zentrale Ansatz des Migrationsleitfadens ist die Hinführung auf offene Standards, sei es im Bereich der Datenhaltung, von Schnittstellen oder von Protokollen. Der Begriff „Offener Standard“ ist keine Schutzmarke und auch sonst nicht rechtlich geschützt; es gibt weder eine allgemeingültige noch eine verbindliche Definition dieses Begriffs. Trotzdem wird er in vielen Verlautbarungen und Dokumenten verwendet und ist beispielsweise ein wiederkehrender Aspekt in verschiedenen Beschlüssen des IT-Rats.

Letztere beziehen sich dabei implizit auf den SAGA-Standard, der zwar keine Definition offener Standards enthält, aber folgende Mindestanforderungen an die Offenheit von Spezifikationen definiert (Die11a):

„Die Mindestanforderungen bezüglich der Offenheit sind:

1. Die Spezifikation wurde vollständig publiziert und die Publikation ist entweder kostenfrei oder gegen ein angemessenes Entgelt erhältlich.
2. Die Verwendung der Spezifikation ist für Hersteller und Nutzer der Software-Systeme uneingeschränkt und kostenfrei möglich.
3. Zum Zeitpunkt der Bewertung ist nicht erkennbar, dass die Spezifikation in der Zukunft die ersten zwei Anforderungen nicht mehr erfüllen wird.“

Im Entwurf zur kommenden Version des Europäischen Interoperabilitätsrahmens (EIF) wird die Offenheit von Spezifikationen abweichend definiert (Eur10)[2]:

„If the openness principle is applied in full:

1. All stakeholders have the same possibility of contributing to the development of the specification and public review is part of the decision-making process;
2. The specification is available for everybody to study;
3. Intellectual property rights related to the specification are licensed on FRAND."[3]

Diese Definition erlaubt also Spezifikationen auf der Basis geschützter Patente und eine Gebühr für deren Nutzung, wenn auch unter der Bedingung, dass sie fair, angemessen und nicht diskriminierend sein muss (FRAND). Das steht im Gegensatz zur SAGA-Definition, in der lediglich eine angemessene Gebühr für den Bezug der Spezifikations-Dokumentation erlaubt ist, die Verwendung und Implementierung des darin beschriebenen Standards hingegen uneingeschränkt und kostenfrei zu sein hat. Der EIF-Ansatz wird daher im Migrationsleitfaden nicht weiter berücksichtigt.

Die am weitesten gehende Definition offener Standards wurde von der Free Software Foundation Europe (FSFE) auf der Basis der ersten Version des EIF entwickelt[4]:

„Ein Offener Standard bezieht sich auf ein Format oder Protokoll, das

1. einer vollständig öffentlichen Bewertung und Nutzung unterliegt, ohne Hemmnisse auf eine für alle Beteiligten gleichermaßen zugänglichen Weise,
2. ohne jegliche Komponenten oder Erweiterungen ist, die von Formaten oder Protokollen abhängen, die selbst nicht der Definition eines Offenen Standards entsprechen,
3. frei ist von juristischen oder technischen Klauseln, die seine Verwendung von jeglicher Seite oder jeglichem Geschäftsmodell einschränken,

[2] Das Dokument liegt leider nur in englischer Sprache vor.
[3] FRAND: Fair, reasonable and non discriminatory terms or on a royalty-free basis in a way that allows implementation in both proprietary and open source software.
[4] http://fsfe.org/projects/os/def.html

4. unabhängig von einem einzelnen Anbieter geleitet und weiterentwickelt wird, in einem Prozess, der einer gleichberechtigten Teilnahme von Wettbewerbern und Dritten offen steht,
5. verfügbar ist in verschiedenen vollständigen Implementierungen von verschiedenen Anbietern oder als vollständige Implementierung gleichermaßen für alle Beteiligten.“

Diese Definition enhält mit der Verfügbarkeit von Implementierungen und der Unabhängigkeit von einzelnen Anbietern gegenüber den anderen betrachteten Ansätzen neue Aspekte. Auch die sonstigen Punkte gehen teilweise über die SAGA-Mindestanforderungen hinaus. Insgesamt sind die Formulierungen so gewählt, dass Abhängigkeiten von Herstellern, Patenten oder nicht-offenen Standards wirksam verhindert werden.

Wenn im Migrationsleitfaden von einem offenen Standard die Rede ist, bezieht er sich daher stets auf die im SAGA-Standard enthaltenen Mindestanforderungen an die Offenheit und berücksichtigt zudem die weitergehenden Aspekte der FSFE-Definition.

## 2.3 Konformität und Interoperabilität

Konformität ist die Beziehung zwischen einem Produkt und einem Standard. Ein Produkt ist standardkonform, wenn es sowohl die obligatorischen Anforderungen des Standards als auch die umgesetzten optionalen Anforderungen einhält (OAS10). Ein Standard sollte möglichst so gestaltet sein, dass die Konformität eines Produkts automatisiert und wiederholbar geprüft werden kann.

Gemäß ISO/IEC 2382-01 “Information Technology Vocabulary, Fundamental Terms” bezeichnet Interoperabilität die Fähigkeit, zwischen verschiedenen funktionalen Einheiten zu kommunizieren, Daten auszutauschen oder Programme auszuführen, ohne dass der Anwender die spezifischen Charakteristika dieser Einheiten näher kennen muss. SAGA definiert Interoperabilität als „Fähigkeit von Informationssystemen, Daten auszutauschen und Wissen zu teilen“[5].

Standardkonformität ist eine notwendige, aber keine hinreichende Voraussetzung für die Interoperabilität von Software-Systemen, da eine vollständige und zweifelsfreie Definition aller Aspekte der Interaktion funktional unabhängiger Einheiten praktisch nicht geleistet werden kann. Beispielhaft sei die teils sehr unterschiedliche Darstellung desselben Dokuments durch verschiedene Office-Suiten genannt. Daher ist das Vorliegen einer Open-Source-Referenzimplementierung des jeweiligen Standards von Vorteil, die im Zweifel entsprechend analysiert und zur weiteren Konkretisierung des Standards oder als Vorlage für weitere Implementierungen desselben verwendet werden kann. Zertifizierungen von Software über die Einhaltung bestimmter Standards durch erfolgreiches Bestehen definierter Testläufe sind eine weitere Möglichkeit, die Konformität nachzuweisen.

Der Java Community Process[6] ist ein Beispiel für solche Zertifizierungen. Er kombiniert einen bestimmten Standard (Java Specification Request (JSR)) mit einer Referenzimplementierung (RI) und einem Testverfahren (Technology Compatibility Kit) zur Prüfung der Konformität von Java-Implementierungen gegen den konkreten Standard. Durch diese Kombination und die strikte Einhaltung des Prozesses wird gewährleistet, dass Java-Implementierungen weitestgehend miteinander kompatibel sind und die geprüften Standards einhalten.

[5] siehe (Die11a), Kap. 3.5
[6] http://jcp.org/

## 2.4 Schnittstellen, Module, Komponenten und Services

Modularisierung verringert die Komplexität der Bestandteile eines Gesamtsystems durch deren Aufteilung und die Festlegung klarer Grenzen zwischen ihnen. Die Ideen dazu reichen zurück bis in die 1970er Jahre, in denen David Parnas das Modulkonzept entwickelte. Ein modulares System zeichnet sich durch hohe Kohäsion und schwache Kopplung aus, also durch die Strukturierung nach enger inhaltlicher Zugehörigkeit in kleinen Einheiten, deren Implementierung nach außen nicht sichtbar ist und die über klar definierte Schnittstellen genutzt werden.

Schnittstellen können vielgestaltig und auf verschiedenen Abstraktionsebenen auftreten. Je abstrakter eine Schnittstelle gestaltet ist, desto unabhängiger sind deren Implementierungen von einer bestimmten Technologie. Weitgehend abstrakte Schnittstellen sind beispielsweise standardisierte Dateiformate und Anwendungsprotokolle wie das Hypertext Transfer Protocol (HTTP), während konkrete und damit technologisch einengende Schnittstellen beispielsweise bei der Nutzung dynamischer Bibliotheken über binäre Funktionssignaturen auftreten.

Komponenten kombinieren verschiedene Module zu funktionalen Einheiten einer höheren Ebene, beispielsweise zur Abbildung eines fachlichen Einsatzbereichs. Sofern sie selbst wiederum von außen angesprochen werden sollen, geschieht dies ebenfalls in Form von Schnittstellen. Die über diese Schnittstellen angebotene Funktionalität wird als Service bezeichnet. Komponenten und Services verbergen nach außen die enthaltenen Module und deren Art der Zusammenarbeit und entsprechen damit ebenfalls den Prinzipien der Modularisierung.

Durch die Kommunikation über abstrakte, standardisierte Schnittstellen werden ungewollte Abhängigkeiten zwischen Modulen, Komponenten oder Services verringert und alternative Entwicklungen ermöglicht. Daher sind nach diesen Prinzipien modularisierte Systeme leichter wart- und erweiterbar; Änderungen sind besser lokalisierbar und haben weniger Seiteneffekte auf das Gesamtsystem. Sie ermöglichen ein leichter änderbares Verhalten und erlauben die Integration verschiedener Implementierungen derselben Schnittstelle. Das Paradigma Service-orientierter Architekturen (SOA) basiert beispielsweise ebenso auf diesen Prinzipien wie Browser-Plug-Ins oder der Zugriff auf Verzeichnisdienste über das Lightweight Directory Access Protocol (LDAP).

## 2.5 Integration

Eine der zentralen Aufgaben beim Aufbau und Betrieb von Informationstechnologie besteht darin, das Zusammenspiel der verschiedenen Software-Komponenten möglichst reibungslos zu gestalten und dadurch die Effektivität des Gesamtsystems zu optimieren. Je mehr die Teilsysteme unmittelbar miteinander interagieren, desto höher ist der Grad der Integration.

Die Integration von Teilsystemen ist in Behörden vielfach ein kontinuierlicher Vorgang; Komponenten müssen erneuert, erweitert oder an neue Anforderungen angepasst werden. Da mit jeder Integration Aufwand und Risiko verbunden sind, werden die zu integrierenden Teilsysteme meist so ausgewählt, dass sie sich möglichst nahtlos in die vorhandene Umgebung einbinden lassen.

### 2.5.1 Integrationsformen

Am Markt haben sich verschiedene Formen der Software-Integration herausgebildet, die in Aufwand und Bedeutung hinsichtlich der Abhängigkeit von Produkten oder Herstellern stark variieren.

#### 2.5.1.1 Zusammenstellungen

Die für die Nutzung verschiedener Produkte am wenigsten aufwendige Integrationsform ist der Bezug konfektionierter Software-Pakete, deren Komponenten bereits für ein reibungsloses Zusammenspiel konfiguriert sind. Bekannte Beispiele dafür sind XAMPP[7], Appliances[8] und die Cloud-Computing-Variante *Platform as a Service (PaaS)*.

Der Anwender erhält damit ein funktionierendes System mit einem definierten Satz an Eigenschaften, ohne dass er die Details des Zusammenspiels der einzelnen Komponenten kennen muss. Die Bestandteile eines solchen Software-Pakets sind regelmäßig auch separat erhältlich, die Paketierung erspart allerdings die manuelle Installation der einzelnen Komponenten und deren jeweilige Konfiguration, ohne die Flexibilität der einzelnen Komponenten oder des Gesamtsystems einzuschränken.

Zusammenstellungen haben einen definierten Verwendungszweck, können aber aufgrund der schwachen Kopplung der Komponenten für andere Zwecke angepasst oder erweitert werden.

#### 2.5.1.2 Funktionale Integration

Eine funktionale Integration besteht, wenn Funktionen einer Softwarekomponente durch andere Komponenten verwendet werden. Dazu zählen beispielsweise eine Service-orientierte Architektur (SOA) mit ihren bereitgestellten und verknüpften Services, die Nutzung dynamischer Bibliotheken, Browser-Plug-Ins oder die aus dem Bereich von Office-Paketen bekannten OLE-Verknüpfungen. Sie unterscheiden sich in der Abstraktionsebene der Schnittstelle, die vom unmittelbaren Verwenden fremden Maschinencodes über proprietäre Schnittstellen bis zum Austausch von XML-Daten reicht. Die Verwendung proprietärer Schnittstellen bringt technologische Abhängigkeiten mit sich und ist ein Merkmal stark integrierter Komponenten. Sie entspricht im Sinne der Modularisierung einer starken Kopplung und widerspricht damit deren Zielen. Schnittstellen auf höheren Abstraktionsebenen entsprechen hingegen der losen Kopplung und sind daher zugunsten einer möglichst weitgehenden technologischen Unabhängigkeit vorzuziehen.

#### 2.5.1.3 Datenintegration

Bei der Datenintegration greifen mehrere Anwendungen oder Services auf dieselben Daten zu, wodurch Redundanzen in der Datenhaltung vermieden werden sollen. Wie bei der funktionalen gibt es auch bei der Datenintegration verschiedene Grade. Der unmittelbare Zugriff mehrerer Anwendungen auf dasselbe Datenbankschema ist vergleichbar mit der Verwendung proprietärer Schnittstellen und

[7] Komplettinstallation eines Apache, MySQL, PHP und Perl Servers auf verschiedenen Plattformen, http://www.apachefriends.org/de/xampp.html

[8] Bezug z.B. vom VMware Virtual Appliance Marketplace http://www.vmware.com/appliances

entspricht einer starken Kopplung. Greifen die Anwendungen hingegen über abstrakte Zugriffsschichten wie Objekt-relationale Mapper oder Dienste auf die Daten zu, sind sie von den physikalischen Datenstrukturen entkoppelt. Eine solche Entkopplung vermeidet Inkonsistenzen und unerlaubte Zugriffe und kann auch als Transformationsschicht für unterschiedliche Datenmodelle genutzt werden. SAGA empfiehlt den Zugriff auf Daten über bestimmte offene Standards (siehe (Die11b), Kap. 9).

#### 2.5.1.4 Kombinierte Integration

Die zunehmende Service-Orientierung in Software-Architekturen verwischt die Grenze zwischen der funktionalen und der Datenintegration mehr und mehr. Während in früheren Architekturen der unmittelbare Datenzugriff und die Verwendung konkreter, proprietärer Schnittstellen üblich war, verwenden modernere Ansätze Services, die mit datenbezogener Funktionalität und abstrakten Schnittstellen aufwarten. Beispiele dafür sind der XÖV-Standard oder Verzeichnisdienste, die an zentraler Stelle Informationen über Benutzer und deren Rechte und Rollen bereithalten und von anderen Komponenten zur Authentifizierung und Authorisierung des Anwenders über entsprechende Funktionen des offenen Standards LDAP genutzt werden.

Die lose gekoppelte Funktions- und Datenintegration ist ein wesentliches Ziel der Konsolidierung von Standard- und Fachanwendungen.

### 2.5.2 Integrationshilfen

Systeme, die aus miteinander integrierten Softwarekomponenten bestehen, müssen in der Regel mithilfe einer Reihe von Parametern konfiguriert werden können. Das Ändern eines bestimmten Parameters betrifft dabei oft mehrere der integrierten Komponenten. Daher sind Mechanismen hilfreich, die sicherstellen, dass solche Änderungen von Konfigurationsparametern die Integrität des Gesamtsystems nicht stören und alle relevanten Komponenten entsprechend rekonfiguriert werden. Herstellerspezifische Integrationshilfen sind häufig auf die Integration eigener Komponenten beschränkt. Vor dem Einsatz solcher Integrationshilfen sollte daher geprüft werden, ob die Auswahl zu integrierender Komponenten auf der Einhaltung proprietärer oder standardisierter Schnittstellen und Protokolle basiert und ob weitere Einschränkungen vorliegen.

### 2.5.3 Integration und Standardisierung

Jede Form der Integration erfordert Schnittstellen, welche die Kommunikation der beteiligten Komponenten miteinander ermöglichen. Sind diese Schnittstellen nicht offengelegt, ist eine Integration alternativer Lösungen nur schwer möglich. Die Folgen sind eine eingeschränkte Auswahl integrierbarer Komponenten, die Bindung an die Produktfamilie und deren Hersteller, die Unterbindung von Wettbewerb und unnötig hohe Beschaffungskosten. Letzteres kann man beispielsweise der Urteilsbegründung des EuGH in Sachen Microsoft vs. EU-Kommission zum Monopolmissbrauch entnehmen (Eur07). Komponenten mit Schnittstellen auf der Basis offener Standards (siehe 2.2) sind daher in jedem Fall vorzuziehen, deren Unterstützung sollte im Beschaffungsprozess entsprechend berücksichtigt und insbesondere in Ausschreibungen gefordert werden.

### 2.5.4 Integration und Abhängigkeit

Der wesentliche Vorteil integrierter Lösungen besteht darin, dass die einzelnen Komponenten aufeinander abgestimmt sind und ohne großen Aufwand sofort miteinander funktionieren. Hersteller und Distributoren achten bei der Weiterentwicklung und Pflege der einzelnen Komponenten auf den Erhalt des Integrationsgrads. Aktualisierungen berücksichtigen die integrierten Komponenten und reduzieren dadurch den Konfigurationsaufwand und das Risiko von Fehlfunktionen.

Von der bestmöglichen Integration zur Abhängigkeit ist es allerdings nur ein kleiner Schritt. Mit zunehmendem Integrationsgrad wird die Kopplung zwischen den Komponenten immer stärker und läuft zuneh-

mend den Prinzipien der Modularisierung (siehe 2.4) entgegen. Die Nutzung proprietärer Schnittstellen nimmt zu, die Integration von Komponenten über offene Standards findet nur noch teilweise oder überhaupt nicht mehr statt. Damit steigt die Abhängigkeit von bestimmten technischen Lösungen und deren Herstellern, da nur diese in der Lage sind, alle integrativen Aspekte, insbesondere die zunehmende Vielfalt proprietärer Schnittstellen, während der Weiterentwicklung der Komponenten zu berücksichtigen. Die fehlende Offenlegung von Schnittstellen führt außerdem oft dazu, dass nur die Komponenten desselben Herstellers vollständig miteinander kompatibel sind, während sich die Interoperabilität mit Programmen oder Komponenten anderer Hersteller als schwierig oder unmöglich gestaltet, da sie oft nur spät oder unzureichend über Neuerungen informiert werden. Hoch integrierte Lösungen verlieren ihre wesentlichen Vorteile, wenn einzelne Komponenten durch andere, vom Hersteller nicht dafür vorgesehene Komponenten ausgetauscht werden können. Die Auswahl an alternativen Lösungen nimmt folglich ab, es entsteht eine Abhängigkeit von einem bestimmten Hersteller („Vendor Lock-In“), der darüber auch den Erwerb und Einsatz zusätzlicher Produkte durchsetzen kann.

Ein Beispiel für die durch hohe Integration entstehende Produkt- und Herstellerabhängigkeit ist der von Microsoft mit der Groupware Exchange 2000 eingeführte Zwang zur Verwendung des Verzeichnisdiensts Active Directory (AD) aus demselben Hause, u.a. für die integrierte Verwaltung von Benutzern und Exchange-Konten. Neben den Lizenzkosten entsteht Aufwand für die Konzeption dieses Verzeichnisdienstes, dessen Integration mit bestehenden Identity-Management-Systemen sowie für dessen laufende Administration. Zudem kann das aktuelle Exchange 2010 nur auf einem Microsoft Server 2008 installiert werden, für den weitere Lizenzen und Administrationsaufwand anzusetzen sind. Dem Vorteil einer sehr gut gelösten und hoch integrierten Benutzerverwaltung steht damit die erzwungene Festlegung auf ein bestimmtes Betriebssystem und weitere Produkte desselben Herstellers entgegen.

Dass eine gute Integration auch ohne starke Produkt- oder Herstellerbindung möglich ist, zeigt beispielhaft die Univention GmbH mit ihrem Produkt Corporate Server (UCS). Es besteht aus einer Zusammenstellung von Infrastrukturkomponenten wie Verzeichnis-, Druck-, Anmelde- und Virtualisierungs-Diensten, die jeweils über offene Standards kommunizieren und über ein zentrales Werkzeug administriert und konfiguriert werden. Alle Komponenten sind Open-Source-Software (OSS) und können auch separat genutzt oder durch alternative Implementierungen des jeweiligen Standards ersetzt werden. Beispielsweise können derzeit drei verschiedene Lösungen als Groupware und zwei alternative Virtualisierungstechnologien genutzt werden. Benutzer und Konten werden im Verzeichnisdienst OpenLDAP verwaltet, AD kann über einen Connector ebenso eingebunden werden. Das zentrale Administrationswerkzeug integriert die verschiedenen Dienste und erlaubt dadurch deren gemeinsame Konfiguration. Die zur Anbindung an das zentrale Administrationswerkzeug nötigen Erweiterungen sind ebenfalls als OSS freigegeben und können dadurch als Vorlage für die Einbindung weiterer Komponenten genutzt werden. Durch diese Offenheit entsteht weder eine Produkt- noch eine Herstellerabhängigkeit.

Das auf der OSGi Service Platform (OSGi)[9] basierende Eclipse[10] ist ein weiteres prominentes Beispiel für die Entwicklung einer enormen Vielfalt an gut integrierten Erweiterungen und Produkten durch die Nutzung von OSS auf der Basis offener Standards und hat sich als Plattform für Anwendungen in diversen Branchen etabliert. Die Verwendung von Eclipse reicht vom Einsatz als Entwicklungsumgebung für verschiedene Programmiersprachen über die Erstellung Eclipse-basierter Rich Clients[11] bis zum von Airbus Industries 2004 gegründeten Topcased-Projekt – einer Sammlung von Eclipse-Werkzeugen für die System- und Softwareentwicklung im Bereich komplexer technischer Systeme[12].

[9] Eine Einführung in OSGi bietet beispielsweise (WBB10).
[10] http://www.eclipse.org
[11] Beispielsweise als Warenwirtschaftssystem bei der Hama GmbH & Co. KG, siehe http://www.sigs.de/download/oop_07/teufel%20l%FCbken%20Do3-4.pdf
[12] Weitere Informationen zu Topcased z.B. unter http://heise.de/-1194034

### 2.5.5 Fazit

Offene, standardisierte Schnittstellen und Protokolle sind ein wichtiges Mittel zur Sicherung von Herstellerunabhängigkeit und Flexibilität. Sie bringen dadurch langfristig mehr Vorteile als ein hoher Integrationsgrad. Ist zudem der Quellcode der eingesetzten Produkte offengelegt, können Interessierte die Produkte weiter entwickeln, Erweiterungen einbringen oder alternative Implementierungen realisieren. Die Investitionssicherheit der Produktnutzer wird dadurch maximiert, alle Beteiligten profitieren gleichermaßen von Weiterentwicklungen.

## 2.6 Open-Source-Software

Unter Open-Source-Software (OSS) wird jede Art von Software verstanden, deren Quelltext frei und kostenlos zugänglich ist und deren beliebige Verwendung durch entsprechende Erklärungen der Urheber gewährt wird. Um diese Prinzipien noch deutlicher zu artikulieren, wird solche Software auch freie Software, *Free and Open Source Software (FOSS)* oder *Free/Libre Open Source Software (FLOSS)* genannt. Die beliebige Verwendung der Software schließt neben deren Nutzung auch die Analyse und Änderung mit ein. Die Verbreitung geänderter OSS und die kommerzielle Nutzung ist grundsätzlich möglich, unterliegt allerdings je nach Lizenz bestimmten Auflagen (siehe Kapitel 3.4.2). Die Open Source Initiative (OSI) führt eine Liste aller von ihr anerkannten OSS-Lizenzen (siehe 2.6.4). Prominente Beispiele für OSS sind der Linux-Kernel, der Apache Web Server und der Web Browser Mozilla Firefox.

Viele Hersteller von OSS-Produkten bieten Dienstleistungen zu ihren Produkten an, insbesondere die Übernahme der Gewährleistung, Schulungen, Unterstützungsleistungen oder Service Level Agreements (SLAs). Gängige Modelle für deren Finanzierung sind das Software-Abonnement, welches beispielsweise Gewährleistung oder schnelle Reaktionszeiten beinhalten kann, und das *Dual Licensing*, bei dem der OSS-Bezieher zwischen einer OSS-Lizenz ohne Gewährleistung und sonstige Leistungen sowie einer kommerziellen Lizenz mit entsprechenden Leistungen wählen kann.

### 2.6.1 Standardisierung und Open-Source-Software

Die Entwicklung von OSS ist eng mit der Herausbildung offener Standards verbunden; für die meisten offenen Standards existieren OSS-Referenzprodukte, die diesen Standard beispielhaft und nachvollziehbar umsetzen und damit die Vorlage für alternative, durchaus auch proprietäre Implementierungen bilden.

Standardisierungsprozesse weisen verschiedene Parallelen zu häufig verwendeten Entwicklungsmodellen von Open-Source-Software auf. Viele Open-Source-Projekte mit einer breiten und aktiven Community diskutieren Anregungen und Änderungen über öffentliche Mailinglisten[13] oder Diskussionsplattformen[14]. Die Beteiligung daran ist zwar an gewisse Regeln gebunden (insbesondere sollte man die relevanten bisherigen Beiträge gelesen haben), steht aber allen Interessierten frei. Die Ergebnisse solcher Diskussionen münden ggf. in den ebenfalls frei zugänglichen Source-Code. Dies ist vergleichbar mit Standardisierungsverfahren, bei denen der Standard selbst beziehungsweise die während seiner Entwicklung diskutierten Entwürfe einer (Fach-)Öffentlichkeit verfügbar gemacht und von dieser diskutiert werden.

Hierin besteht allerdings kein Automatismus. Open-Source-Lizenzierung bedeutet nicht zwangsläufig, dass über die Weiterentwicklung des Quellcodes einer Anwendung öffentlich diskutiert werden muss. Der Anwender einer Open-Source-Software erhält allerdings immer das Recht, den zugehörigen Quellcode zu analysieren. Dadurch verfügt er stets über eine eindeutige Beschreibung der von dieser Software verwendeten Protokolle und Schnittstellen nebst ihrer Implementierung. Dies ist ein Vorteil gegenüber proprietärer Software und entspricht einem wichtigen Aspekt von offenen Standards – deren frei zugänglicher und lückenloser Beschreibung. Bei mehrdeutigen Formulierungen eines Standards kann der Open-Source-Lizenznehmer zudem den fraglichen Quellcode analysieren und beispielsweise so verändern, dass die Interoperabilität mit anderen Anwendungen verbessert wird.

### 2.6.2 Open-Core-Software

Als Open-Core-Software (OCS) wird die Kombination aus einem freien OSS-Kernprodukt und proprietären Zusatzfunktionen bezeichnet. Die Zusatzfunktionen betreffen regelmäßig für den Betrieb im professionellen Umfeld notwendige Teile wie uneingeschränkte Benutzerzahlen, Adapter für geläufige proprietäre Software oder Backup- und Recovery-Funktionalität.

[13] Beispielsweise zum Linux-Kernel unter http://vger.kernel.org/
[14] Beispielsweise zu OTRS unter https://otrsteam.ideascale.com

Anbieter von OCS wollen einerseits von den Vorzügen von OSS profitieren und andererseits durch ein traditionelles Lizenzmodell Umsatz durch den Verkauf von Software sowie eine starke Kundenbindung über die proprietären Zusatzfunktionen erreichen. Die wesentlichen Aspekte von OCS sind[15]:

- Der Kern der Software steht unter einer Copyleft-Lizenz (siehe Unterkapitel 3.4) wie der GNU General Public License (GPL).
- Für die Verwendung der Kernkomponenten in einem proprietären Produkt wird eine kommerzielle Lizenz benötigt.
- Gegen Bezahlung werden Zusatzfunktionen und/oder weitere Plattformen für das Kern-Produkt angeboten.

Im Gegensatz zum für OSS gebräuchlichen *Dual Licensing* sind Bezieher von OCS hinsichtlich der proprietären Bestandteile an die Produktpolitik des Herstellers gebunden und können diese Bestandteile meist nicht ohne Weiteres durch OSS-Komponenten ersetzen. Beim Beschaffen von OCS sind daher dieselben Aspekte zu beachten wie für rein proprietäre Software (siehe 2.7).

### 2.6.3 Produkteinsatz

Open-Source-Software erweckt unter anderem die Erwartung, dass sie sich in die Infrastruktur der öffentlichen Verwaltung kostengünstig und sicher einbauen lässt. Tatsächlich sind solche Produkte kostenlos oder paketiert zu einem Bruchteil der Kosten kommerzieller Produkte verfügbar, wodurch sich Mittel für Lizenzkosten einsparen lassen. Die Einführung von Software-Produkten erfordert aber auch im Fall von OSS weitere Mittel, sei es für Anpassungen und Erweiterungen des Produkts selbst, für Anpassungen der übrigen Teilsysteme an das neue Produkt, für Schulungen oder sonstige externe Leistungen. Lizenzkosten können, müssen aber keinen großen Anteil an den insgesamt mit der Produkteinführung verbundenen Kosten haben. Gesparte Lizenzkosten sind daher kein zwingender Grund für die Einführung von OSS.

Die Implementierung offener Standards ist, wie oben dargestellt, im Bereich von OSS die Regel. Offene Standards werden aber auch vielfach von proprietären Produkten implementiert. So entsteht eine Produktvielfalt rund um den jeweiligen Standard, was die Abhängigkeit von einem einzelnen Hersteller wirksam verhindert. Die verschiedenen konkurrierenden Ansätze sorgen zudem für günstige Preise für Dienstleistungen rund um den Standard. Bei OSS-Produkten können darüber hinaus benötigte Dienstleistungen oder Implementierungen von verschiedenen Anbietern bezogen werden, was sich ebenfalls positiv auf die Kosten auswirkt. Durch die bei offenen Standards vorhandene Vielfalt an Produkten, Herstellern und Dienstleistern besteht daher eine langfristige Investitionssicherheit. Offene Standards in der Kombination mit kostenlosen OSS-Lizenzen sind folglich aus wirtschaftlicher Sicht gute Gründe für die Einführung von OSS.

Neben den wirtschaftlichen Aspekten sind Datenschutz und IT-Sicherheit wichtige Kriterien bei der Beurteilung von Software. Wo und in welcher Form welche Art von Daten gespeichert oder weitergegeben werden, welche Möglichkeiten zur Überwachung von Anwendern oder anderen Systemen gegeben sind, ob das Produkt Hintertüren zur unbemerkten Fremdsteuerung oder Datenweitergabe aufweist – all dies kann bei vorliegendem Quellcode und entsprechendem Expertenwissen verifiziert werden. Dadurch ist es auch möglich, die Umsetzung konkreter Datenschutzvorgaben zu überprüfen. Aufgedeckte Fehler und Schwachstellen können selbst bereinigt und das Produkt dadurch gehärtet werden, um es beispielsweise in sicherheitskritischen Umgebungen einzusetzen. Es können beliebige in- und externe Experten auch ohne Hinzuziehung des Herstellers zu sicherheitstechnischen Untersuchungen beauftragt werden. Diese Aspekte sind also ebenfalls gute Gründe für die Einführung von OSS.

Der Migrationsleitfaden betrachtet daher in den Themengebieten des Kapitels 4 jede Produktgattung unter anderem dahingehend, welche offenen Standards für diese Gattung relevant sind, ob die untersuchten Produkte den jeweiligen Standard einhalten und unter welchen Lizenzen sie verfügbar sind.

[15] vgl. (Lam08)

### 2.6.4 Entstehung von OSS

Bis zum Ende der 60er Jahre wurden Computersysteme inklusive der Anwendungen im Quellcode verkauft. Software wurde häufig von den Anwendern selbst geschrieben und anderen zur Verfügung gestellt (Fre01). Es entstand eine Kultur der gegenseitigen Hilfe und des freien Austauschs von Problemlösungen. In den 70er Jahren entwickelte sich ein Markt für Software, und um Eigenentwicklungen zu schützen, wurde der Quelltext von den Herstellern unter Verschluss gehalten. So arbeiteten mehrere Entwicklergruppen isoliert voneinander oft an ähnlichen Problemen. Eine Folge dieses Trends war zum Beispiel die Zersplitterung der Unix-Betriebssysteme in viele zueinander inkompatible Versionen.

Richard Stallman, damals Programmierer am Massachusetts Institute of Technology (MIT), wollte 1984 dieser Entwicklung nicht mehr folgen. Er begann ein eigenes Projekt für ein Betriebssystem unter dem Namen GNU[16]. Jeder sollte dort auf die Quellen zugreifen, sie studieren, erweitern und anpassen können. In Kombination mit dem Linux-Projekt, das der norwegische Student Linus Torvalds 1991 begann, entwickelte sich das heute weit verbreitete GNU/Linux-System. Um die freie Verfügbarkeit seiner Software abzusichern, entwickelte Stallman die GNU General Public License (GPL), die über das Urheberrecht eine Software samt jeglicher Änderung, Erweiterung oder Ableitung dauerhaft frei verfügbar hält. Zudem gründete er 1985 die Free Software Foundation (FSF) als Vertreterin dieser Lizenz und darunter entwickelter Software.

In den neunziger Jahren entwickelte sich die Open-Source-Bewegung weiter und brachte neben GNU/-Linux viele weitere sehr erfolgreiche Projekte hervor. Dabei waren nicht alle so strikter Auffassung wie Stallman. Insbesondere die „virale“ Eigenschaft der GPL, dass alle Änderungen, Erweiterungen und Ableitungen ebenfalls frei sein müssen (das sogenannte Copyleft), wurde von vielen als zu große Einschränkung für eine kommerzielle Nutzung betrachtet. Eric Raymond, der seit den achtziger Jahren aktiv an GNU-Projekten und auch am Mozilla-Projekt mitgearbeitet hatte, setzte sich mit an die Spitze dieser Untergruppe, die 1998, ohne Stallman, die Open Source Initiative gründete. Diese entwickelte eine eigene Open-Source-Definition[17], nach deren Grundsätzen sie Software-Lizenzen überprüft und ggf. als Open-Source-Lizenz anerkennt. Sie hat inzwischen über 70 verschiedene Software-Lizenzen als Open-Source-Lizenzen anerkannt.

[16] GNU ist ein Akronym für „GNU's not UNIX“.
[17] http://www.opensource.org/docs/osd

## 2.7 Proprietäre Software

Proprietäre Software ist unfreie Software, deren Quellcode nicht offenliegt und deren Verbreitung oder Veränderung grundsätzlich nicht gestattet ist. Damit ist die Anpassung des Sourcecodes an eigene Bedürfnisse ebenso wenig möglich wie eine unmittelbare Behebung festgestellter Fehler. Vielmehr ist der Nutzer proprietärer Software abhängig von Fehlerbehebungsintervallen und Produktzyklen des Herstellers. Proprietäre Software wird über das Urheberrecht hinaus häufig durch US-amerikanische Patente geschützt[18], die allerdings derzeit in Europa mangels Patentierbarkeit von Software als solcher kaum durchgesetzt werden können[19].

Proprietäre Software verhindert durch die Überlassung in Binärform ihre unmittelbare Prüfbarkeit auf die Einhaltung von Standards und Datenschutzvorgaben. Die Interoperabilität leidet vielfach an nicht nachvollziehbaren Interpretationen von Standards, eine statische Codeanalyse zur Aufdeckung von Schwachstellen ist nicht möglich. Standardkonformität, Interoperabilität und Sicherheitsrisiken proprietärer Software sind daher wesentlich schwieriger zu bewerten als bei offener Software.

### 2.7.1 Freeware

Kostenlos in Binärform bereitgestellte proprietäre Software wird als *Freeware* bezeichnet. Im Gegensatz zur OSS gewährt der Freeware-Eigentümer lediglich das Recht, die Software in ihrem veröffentlichten binären Zustand zu gebrauchen. Der Quelltext ist nicht frei zugänglich und folglich auch nicht änderbar, das Gebrauchsrecht wird teilweise auf bestimmte Organisationen oder Zwecke eingeschränkt. Es existieren regelmäßig keine Lizenzen, die eine Verbreitung der Software durch andere als den Eigentümer erlauben. Freeware ist daher nicht mit OSS gleichzusetzen, es bestehen deutliche Einschränkungen. Ein prominentes Beispiel für Freeware ist der Adobe Acrobat Reader.

### 2.7.2 Shareware

Sogenannte *Shareware* ist ebenfalls proprietärer Natur. Sie darf zwar regelmäßig in Binärform weiterverbreitet werden, bietet aber meistens einen eingeschränkten Funktionsumfang oder eine zeitliche Begrenzung, um die Software evaluieren zu können. Die dauerhafte und vollumfängliche Verwendung ist mit dem Erwerb einer Lizenz verbunden, der Quelltext ist nicht frei zugänglich und folglich auch nicht änderbar.

[18] Siehe bspw. „Die Auseinandersetzung um das Patentwesen und der Streit über Softwarepatente“ unter http://heise.de/-302334

[19] Zur Ablehnung amerikanischer Schutzansprüche in Europa siehe beispielsweise (Bes11)

# Kapitel 3

# Kriterien für erfolgreiche Migrationen

Für eine erfolgreiche Software-Migration ist die Klärung der technischen Umstände eine notwendige, aber keine hinreichende Bedingung. Vielmehr ist eine Reihe weiterer Kriterien zu beachten, die für einen reibungslosen Migrationsverlauf erfüllt sein müssen. Diese allgemeinen Kriterien werden nachfolgend vorgestellt.

Besonders zu beachten ist der Abschnitt 3.2 zur Vorgehensweise, der für verschiedene Migrationstypen die jeweils relevanten Kriterien und Schritte nennt. Er dient damit als Wegweiser durch die verschiedenen Kriterien dieses Kapitels.

## 3.1 Ziele einer Migration

Vor einer Migration müssen zunächst deren unmittelbare Ziele geklärt werden. Diese leiten sich entweder aus erkannten Schwachstellen oder notwendigen Erweiterungen der Bestandssoftware ab, oder sie sind betriebswirtschaftlicher oder strategischer Natur. Häufige Migrationsziele sind

1. ein verbesserter Anwendernutzen,
2. das Herstellen eines rechtlich notwendigen Zustands,
3. die Behebung von Fehlern,
4. die Erweiterung des Funktionsumfangs,
5. eine verbesserte Integration in die vorhandene Systemlandschaft,
6. eine verbesserte Interoperabilität,
7. eine Verringerung der laufenden Kosten,
8. die Erhöhung der Produktivität,
9. die bessere Nutzung vorhandener Resourcen sowie
10. die Einhaltung strategischer Vorgaben (siehe 3.3).

Nach der Erfassung der jeweiligen Migrationsziele müssen sie gewichtet oder priorisiert werden, da sie die Grundlage für die Auswahl der künftigen Software darstellen. Die nachfolgend dargestellten Aspekte unterstützen die Zielerreichung und können jeweils einem oder mehreren der erfassten Ziele zugeordnet werden.

## 3.2 Vorgehensweise / Migrationsplanung

Es existieren verschiedene Vorgehensmodelle für Software-Migrationen. In einem Beitrag (Win08) zum BMBF-Forschungsprojekt „Flexible Informationssystem-Architekturen für hybride Wertschöpfungsnetzwerke (FlexNet)“ wurden deren wesentliche Aussagen zusammengeführt zu einem Vorgehensmodell, das die verschiedenen Phasen einer Software-Migration anschaulich beschreibt und daher für den Migrationsleitfaden zu Teilen verwendet wird.

Demnach besteht ein Vorgehensmodell aus den Phasen Konzeption, Systemauswahl und Realisierung, unterteilt in Ist- und Soll-Analyse, Vorauswahl und Endauswahl, Vertragsabschluss und Implementierung. Ein Phasenmodell betrachtet den Projektablauf anhand wohldefinierter Abschnittsgrenzen, wobei wohl definiert hier nicht im Sinne der Überschneidungsfreiheit, sondern im Sinne genauer zu spezifizierender Abläufe gemeint ist. Daher können bei den einzelnen Modellphasen Überlappungen auftreten, z.B. bei der Ist-Analyse und der Soll-Konzeption. Auch muss der Ablauf der einzelnen Schritte der Phasen nicht streng sequentiell sein.

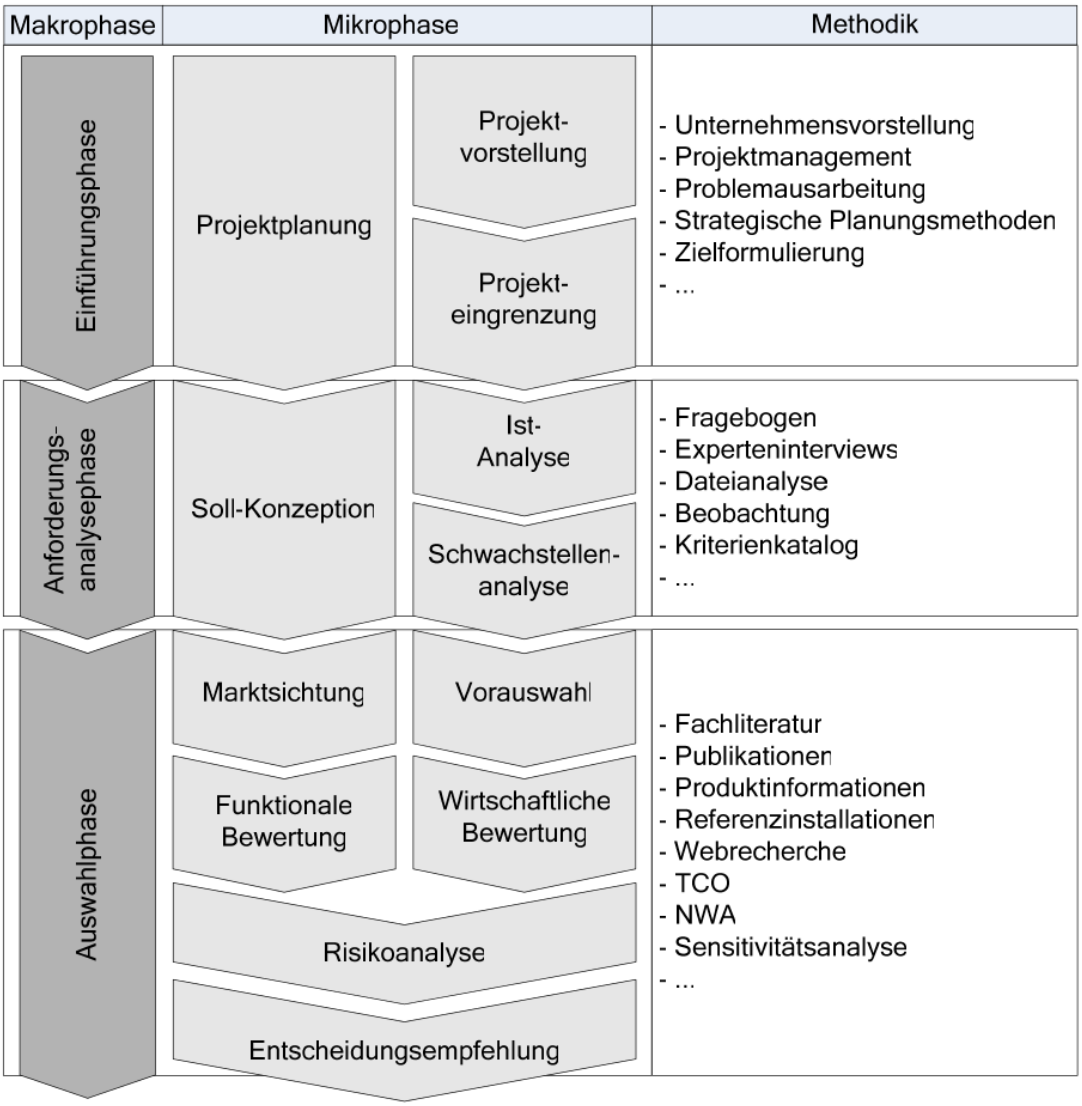


**Abbildung 3.1:** Vorgehensmodell für Software-Migrationen

Das Vorgehensmodell in Abbildung 3.1[1] unterteilt sich in Makrophasen, Mikrophasen und Methodik. Die Makrophasen beschreiben die drei Hauptphasen in diesem Modell. Die Mikrophasen verfeinern die Makrophasen anhand durchzuführender Projektschritte, die parallel oder sequentiell ablaufen können. Neben jeder Mikrophase befindet sich ein Textblock mit möglichen anzuwendenden Methoden für die entsprechende Makrophase.

Das Modell beginnt mit einer projektvorbereitenden Einführungsphase, in der die genaue Planung und Meilensteine gesetzt werden können. Die Anforderungsanalyse als zweite Makrophase beschäftigt sich detaillierter mit der Behörde und den gestellten Anforderungen aus Behördensicht und ist die Grundlage für die Herangehensweise in den einzelnen Technologiefeldern des Kapitels 4. Die darauf folgende Auswahlphase umfasst den Kern des Entscheidungsproblems – den Vergleich und die Bewertung verschiedener Produkte des jeweiligen Migrationsgebiets sowie daraus resultierender Empfehlungen. Die Umsetzung als letzte Phase geht auf die verschiedenen Migrationswege und deren Auswirkungen ein.

### 3.2.1 Einführungsphase

Der Migrationsfaden beschreibt nachfolgend das Vorgehen bei einer Software-Migration. Für eine Migration müssen einige Voraussetzungen erfüllt sein:

- Die Notwendigkeit einer Software-Migration ist in der Behörde gegeben.
- Die Gründe dafür sind dem IT-Entscheider grundsätzlich bekannt.
- Über die IT-Planung sind bereits Haushaltsmittel veranschlagt.
- Es handelt sich nicht um eine Aktualisierung (siehe Abschnitt 2.1.1).

Der IT-Entscheider muss nun einige Schritte veranlassen, um aus diesen Voraussetzungen ein Vorhaben zu formen. Zunächst ist das Vorhaben mit einem griffigen Namen zu versehen; Pseudonamen mit angehängtem „neu“ o.ä. sind zu vermeiden. Sodann müssen die ggf. nur oberflächlich bekannten Gründe konkretisiert und gewichtet werden. Aus den gewichteten Gründen sind die unmittelbaren Ziele der Migration und ihre jeweilige Priorität herzuleiten. Dazu müssen die in 3.1 genannten beispielhaften Ziele auf den konkreten Fall angepasst und die jeweiligen Spezifika beschrieben werden. Zudem sind wesentliche Auswirkungen auf die Interoperabilität mit anderen in- und externen Systemen abzuschätzen und das Migrationsvorhaben von anderen IT-Projekten und organisatorischen Veränderungen abzugrenzen.

Die wichtigsten Rollen im Migrationsvorhaben müssen festgelegt und mit geeigneten Personen besetzt werden. Das ggf. vorhandene IT-Architekturmanagement ist bei jedem Migrationsvorhaben einzubeziehen. Sofern die Migration von zentraler Bedeutung ist oder wesentliche Elemente des derzeitigen Gesamtsystems beeinflusst, ist auch die Behördenleitung zu involvieren und das Vorhaben behördenweit abzustimmen. Einbeziehung und Abstimmung sind dauerhaft anzulegen, beispielsweise durch regelmäßige Statusbesprechungen, um eine langfristige Unterstützung und Aufmerksamkeit der Leitungsebene für das Vorhaben zu gewinnen und es transparent voranzutreiben.

Das V-Modell XT Bund (Der10) enthält im Teil 1 unter „3.2 Projektgenehmigung und Projektstart“ eine Beschreibung der für die Einführungsphase notwendigen Produkte[2]. Zwar liegt der Schwerpunkt des V-Modells in der Systementwicklung, doch kann die Beschreibung analog auf Migrationsvorhaben angewandt werden. Die Definition des dort genannten Produkts „Projektauftrag“ fasst einige der o.g. und weitere Aspekte folgendermaßen zusammen:

> „Der Projektauftrag schafft die grundlegenden organisatorischen und rechtlichen Rahmenbedingungen für die Projektdurchführung. Das Dokument benennt den Projektleiter, den Projektmanager sowie den Lenkungsausschuss und definiert die Ziele, den Zeitrahmen und das Budget.“

[1] Siehe (Win08), Seite 6

[2] Ein Produkt im Sinne des V-Modells ist ein Ergebnis einer Projektphase, beispielsweise ein bestimmtes Dokument.

Der Projektauftrag bildet die Grundlage des weiteren Vorgehens und ist je nach Relevanz und Auswirkungen des Migrationsvorhabens von der Behördenleitung oder vom IT-Entscheider zu erteilen.

### 3.2.2 Anforderungsanalysephase

Die Anforderungsanalysephase beginnt mit erteiltem Projektauftrag. Je nach Größe des Vorhabens sind ein Projektbüro zur Unterstützung der Projektleitung einzurichten und geeignete Personen für die Anforderungsanalyse zu bestimmen. Das Vorgehen bei der Anforderungsanalyse ist spezifisch für die einzelnen Technologiefelder in den einzelnen Abschnitten des Kapitels 4 beschrieben, unterschieden in die Analyse des Ist- und die Konzeption des Soll-Zustands. Die grundlegenden Aspekte dieser Phase sind nachfolgend stichpunktartig aufgeführt:

1. Ist-Analyse vorbereiten
   (1) Projektbüro einrichten
   (2) Analysephase feinplanen
   (3) Prüflisten, Fragebögen, etc. für die Ist-Analyse erstellen
   (4) Interviewpartner bei vielen betroffenen Anwendern in Gruppen einteilen
   (5) Analysten zu Interviewpartnern / Gruppen zuordnen
2. Ist-Analyse durchführen und folgende Aspekte erfassen:
   (1) Derzeit eingesetzte Software samt Version und genutzten Komponenten
   (2) Genutzte Funktionalität, festgestellte Probleme und Funktionslücken
   (3) Standard-Datenformate und zusätzlich benötigte Formatunterstützung für Abwärtskompatibilität oder Export
   (4) Erweiterungen (Plug-Ins), Eigenentwicklungen u.ä.
   (5) Domänenspezifische Bewertungskriterien
   (6) Relevanz und Priorität einzelner Aspekte
3. Ist-Analyse auswerten
   (1) Gewonnene Erkenntnisse konsolidieren und strukturieren
   (2) Liste mit Mindest-Anforderungen an die Basisfunktionalität erstellen
   (3) Liste mit spezifischen Zusatz-Anforderungen erstellen
4. Soll-Konzeption durchführen
   (1) Aus Ist-Analyse gewonnene Anforderungen prüfen und um fehlende, ggf. domänenspezifische Aspekte ergänzen
   (2) Einzelne Anforderungen dem umsetzenden Teilsystem zuordnen und ggf. von parallelen Vorhaben abgrenzen
   (3) Einzuhaltende offene Standards festlegen
   (4) Ggf. Externe über künftige Standards frühzeitig informieren
   (5) Weiterverwendung vorhandener Erweiterungen und Eigenentwicklungen klären
   (6) Ggf. Übergabe von Eigenentwicklungen an IT-Betrieb planen
   (7) Anforderungen priorisieren

Das Resultat der Analysephase ist eine Beschreibung der funktionalen und nichtfunktionalen Anforderungen an das künftige System sowie eine Skizze der Gesamtsystemarchitektur. Es entspricht dem Produkt „Anforderungen (Lastenheft)“ des V-Modells[3].

[3] Siehe (Der10), Teil 5 Nr. 3.6.5

### 3.2.3 Auswahlphase

Anhand der erstellten und priorisierten Anforderungen müssen nun die grundsätzlich in Frage kommenden Alternativen des jeweiligen Technologiefelds bestimmt werden (Marktsichtung und Vorauswahl). Diese sind anhand der Anforderungen miteinander zu vergleichen, um das Produkt mit der größtmöglichen Anforderungsabdeckung zu ermitteln.

Für wichtige Technologiefelder enthält der Migrationsleitfaden im Kapitel Migrationsgebiete eine Vorauswahl an Produkten, einen Vergleich anhand der für die jeweilige Technologie wichtigsten funktionalen Bewertungskriterien und daraus abgeleiteten Empfehlungen. Die Bewertungskriterien müssen um domänenspezifische Aspekte ergänzt und in ihrer Wertigkeit gewichtet werden, um ein für die konkrete Situation belastbares Gesamtergebnis zu erhalten. Zudem müssen die in den Abschnitten Strategische Aspekte und Sicherheitsaspekte genannten Kriterien bewertet und angemessen gewichtet werden. Die Empfehlungen helfen bei der Wahl zwischen ähnlich bewerteten Alternativen.

Bei Migrationen von Fachverfahren, die selbst oder im Auftrag entwickelt werden, sind außerdem Qualitative Aspekte zu bewerten. Diese Kriterien können im Zweifel auch bei Migrationen zu Standard-Produkten angelegt werden.

Das so ausgewählte Produkt muss in seiner Wirtschaftlichkeit bewertet werden. Die wichtigsten Punkte dazu sind in Abschnitt Wirtschaftliche Aspekte beschrieben. Der Abschnitt enthält zudem einen Verweis auf ein Begleitdokument mit einer detaillierten Wirtschaftlichkeitsbetrachtung für Migrationen.

Schließlich sind die mit einer Migration verbundenen Risiken abzuschätzen. Hierzu sind die Umsetzbarkeit der Anforderungen zu bewerten[4], Rechtliche Aspekte von Software-Migrationen zu betrachten und die allgemeinen Risiken des Projektgeschäfts wie Personalfluktuation, unerwartete technische Schwierigkeiten oder steigende Kosten zu berücksichtigen.

Bei Software-Migrationen müssen zudem die Auswirkungen der Veränderungen auf Anwender und Systembetrieb sowie deren Wechselbereitschaft eingeschätzt und ggf. aktiv gefördert werden, insbesondere durch frühzeitige und regelmäßige Informationen über das Vorhaben und dessen Hintergründe. Die wesentlichen Kriterien hierzu sind in den Abschnitten Aspekte des Systembetriebs und Organisatorische Aspekte dargestellt. Die Beachtung dieser Kriterien senkt das Risiko mangelnder Akzeptanz oder Ablehnung des Migrationsvorhabens durch die Betroffenen.

### 3.2.4 Umsetzung

Die getroffene Entscheidung wird umgesetzt durch die Einführung der neuen Software und die Ablösung der alten. Dabei sind verschiedene Wege möglich (siehe Abschnitt 2.1.4): die Stichtagsumstellung oder die schrittweise Migration.

#### 3.2.4.1 Stichtagsumstellung

Die Stichtagsumstellung bietet eine Reihe von Vorteilen. Einem überschaubaren Planungszeitraum folgt ein eindeutiges, vorab festgelegtes Ende der Umstellungsphase, es besteht keine Notwendigkeit für einen lang anhaltenden Parallelbetrieb verschiedener Systeme, die Kosten einer solchen Migration lassen sich relativ einfach berechnen, die nötigen organisatorischen Schritte gut terminieren. Die Administratoren und Benutzer werden zwar intensiv, dafür aber nur einmal mit Neuerungen konfrontiert. Zudem müssen sich erstere nicht über längere Zeiträume mit der Komplexität paralleler oder heterogener Welten auseinandersetzen.

Eine Stichtagsumstellung birgt allerdings hohe Anforderungen an die Organisation des Projekts und der betroffenen Behörde, an die Technik und an die Finanzen. Die Projektplanung verdichtet sich zum Umstellungszeitraum hin stark, alle zur Durchführung notwendigen Schritte müssen bedacht und eingeplant und die Verfügbarkeit der Projektmitarbeiter für zu erwartende Lastspitzen über das normale Arbeitspen-

[4] vgl. (Der10), Teil 5 Nr. 3.6.6 Anforderungsbewertung

sum hinaus gewährleistet sein. Zeitliche Puffer für unerwartete Ereignisse sind nur in geringem Umfang möglich, Abweichungen von der Planung führen schnell zum (vorläufigen) Scheitern der Umstellung.

Die Behörde muss eine schnelle und punktgenaue Qualifizierung ihrer Mitarbeiter organisieren, damit diese weiterhin ihren täglichen Pflichten nachgehen können und Störungen des Behördenbetriebs minimiert werden. Es müssen auf einen zeitlichen Punkt konzentrierte Umstellungs- und Rollout-Konzepte entwickelt, alle Betroffenen frühzeitig informiert und zur Unterstützung des Vorhabens motiviert werden. Die benötigten Finanzmittel müssen innerhalb eines kurzen Zeitraums verfügbar sein, die in die Mittelfreigabe einzubeziehenden Stellen sollten rechtzeitig informiert und ggf. für eine beschleunigte Bearbeitung motiviert werden.

Stellt das künftige System erhöhte Anforderungen an die vorhandene IT-Infrastruktur oder die Ausstattung der Arbeitsplätze, müssen die künftig benötigten Ressourcen rechtzeitig beschafft und bereitgestellt werden. Je nach Beschaffungsvolumen sind entsprechend lange Ausschreibungszeiträume einzuplanen. Außerdem müssen die beschafften Ressourcen bestmöglich für die Aufnahme in das Gesamtsystem vorbereitet und insbesondere Betriebssysteme, Basis- und Fachanwendungen mit dem jeweils aktuellen Stand rechtzeitig vor dem Umstellungszeitraum aufgespielt werden. Hierfür sind ggf. zusätzliche Software-Lizenzen notwendig, die ebenfalls rechtzeitig beschafft werden müssen.

Die Hauptlast einer Stichtagsumstellung tragen die Administratoren und Anwender – umso mehr, je weniger Know-how bezüglich der neuen IT-Landschaft bei ihnen vorhanden ist. Zwar müssen sich die Administratoren nicht über einen längeren Zeitraum mit verschiedenen IT-Ausrichtungen auseinandersetzen und können sich schon bald ausschließlich auf die neuen Systeme konzentrieren. Doch müssen sie viel Geduld und Überzeugungswillen aufbringen, bis alle Betroffenen effizient mit der neuen Technik umgehen können und die durch den Wechsel bedingten Schwierigkeiten ausgeräumt sind.

Für eine Stichtagsumstellung sollte daher eine überschaubare und nicht übermäßig verzahnte Systemlandschaft vorliegen, in der nur wenige Anwendungen und Dienste für die Aufgabenerfüllung eingesetzt werden. Dies kann bei großen Behörden mit wenigen Server-basierten Fachanwendungen genauso der Fall sein wie bei kleineren Behörden mit Standardbüromitteln. Auch hier kann ein leistungsstarkes IT- oder übergreifendes Architekturmanagement in der jeweiligen Behörde helfen. Des Weiteren sollten unter den Administratoren bereits erste Erfahrungen mit dem Migrationsziel vorliegen, ggf. aus anderen Teilsystemen oder dem privaten Umfeld. Das kann durch frühzeitige detaillierte Informationen und entsprechende Fortbildungen gefördert werden. Schließlich sollte bei der Mehrzahl der Betroffenen eine gewisse Offenheit für Neuerungen vorhanden sein, die die Ablehnung von Änderungen überwiegt.

Sind diese Voraussetzungen gegeben, stellt die Stichtagsumstellung ein sinnvolles Vorgehen dar. Andernfalls ist es empfehlenswert, die Umstellung schrittweise anzugehen.

#### 3.2.4.2 Schrittweise Migration

Bei einer schrittweisen Migration können Behörden und Verwaltungen die notwendigen Kosten der Haushaltslage angepasst verteilen. Fehlendes Know-how kann sukzessive aufgebaut werden. Bestehende Widerstände können langsam abgebaut und Vorbehalte aufgelöst, komplexe IT-Strukturen Stück für Stück zerlegt und neu aufgebaut werden. Die Aufteilung der Migration vieler Arbeitsplätze in kleinere Lose reduziert die Anforderungen an die Anwenderbetreuung und die Systemadministration. Mit jedem erfolgreich absolvierten Schritt steigt die Motivation der Projektbeteiligten, sie gewinnen zudem an Erfahrung und können die bisherigen Prozesse verbessern. Die Anwender wiederum werden nicht mit zu vielen gleichzeitigen Änderungen überfordert.

Allerdings ist ein hoher Planungsaufwand vonnöten, der sich über einen langen Zeitraum erstreckt und kontinuierlich an den Projektverlauf angepasst werden muss. Bei jedem einzelnen Migrationsschritt können unerwartete Schwierigkeiten auftreten oder aufwendige Zwischenmaßnahmen notwendig werden, die den weiteren Migrationsverlauf hemmen können. Die Administratoren und Anwenderbetreuer müssen über den gesamten Zeitraum hinweg ein heterogenes Gesamtsystem abdecken. Die Akzeptanz des Gesamtvorhabens hängt bei allen Beteiligten stark vom Erfolg der ersten für sie spürbaren Schritte ab. Anfängliche Fehlschläge können schnell zu einem negativen Gesamteindruck führen und die Akzeptanz

deutlich verringern. Bei einer langen Gesamtlaufzeit muss auch verstärkt mit Wechseln beim Projektpersonal gerechnet werden, was Übergabe- und Einarbeitungsaufwand mit sich bringt und auch taktische oder strategische Änderungen zeitigen kann. Die Unterstützung des Vorhabens durch die Leitungsebene kann über die Projektzeit durch geänderte Rahmenbedingungen abnehmen oder der Mittelzufluss durch wechselnde politische Prioritäten schwanken.

Eine schrittweise Migration empfielt sich, wenn mehrere funktionale Einheiten oder eine große Zahl von Arbeitsplätzen migriert werden sollen. Zwar ist der Projekterfolg auch bei dieser Vorgehensweise nicht garantiert, doch kann entspannter auf einzelne Schwierigkeiten reagiert werden. Planung und Prozesse können stetig optimiert und an das konkrete Projektumfeld angepasst werden.

Bei der Migration einzelner Produkte sollte eine schrittweise Migration nicht vorschnell als irrelevant ausgeschlagen werden, da es einerseits auf die Art der Migration ankommt (siehe 2.1) und andererseits ggf. die Vielzahl umzustellender Einzelsysteme mit einer entsprechend stark ansteigenden Zahl von Support-Anfragen verbunden sein kann, die zeitlich verteilt werden muss, um die Anwenderunterstützung nicht zu überfordern.

Allerdings sollte das Vorhaben zeitlich nicht überstrapaziert werden, um Langläufer-Probleme wie sich ändernde Leitungsvorgaben oder Personalwechsel zu vermeiden. Auch sollten nicht zu viele funktionale Einheiten in die Migrationsplanung aufgenommen, sondern ggf. in mehrere sich überlappende Migrationen mit je eigenem Projektteam aufgeteilt werden. Das bringt zwar zusätzlichen Abstimmungsaufwand mit sich, vermeidet aber die Überforderung eines einzelnen Projektteams und bietet die Möglichkeit zu klaren Abgrenzungen des Projektauftrags.

### 3.2.5 Kompetenzzentrum Open-Source-Software

Das Kompetenzzentrum Open-Source-Software (CC OSS)[5] in der Bundesstelle für Informationstechnik des Bundesverwaltungsamtes fördert den Einsatz von offenen Standards und Open-Source-Software (OSS) in der Bundesverwaltung. Interessierten Bundesbehörden bietet das CC OSS Hilfestellung bei den wesentlichen OSS betreffenden Belangen. Dazu gehört insbesondere die Beratung von der Entscheidungsfindung über die Produktauswahl bis zur Migrationsberatung. Außerdem pflegt das Kompetenzzentrum OSS ein Netzwerk von Erfahrungsträgern und kann darüber Ansprechpartner für gezielte Fragestellungen vermitteln.

[5] http://www.oss.bund.de/

## 3.3 Strategische Aspekte

Bei der Migrationsplanung sind neben den unmittelbaren Zielen (siehe 3.1) auch strategische Erwägungen einzubeziehen. Bundesbehörden stehen im regen Datenaustausch mit anderen Behörden, mit Wirtschaftsbeteiligten und mit Bürgern. Die IT-Rahmenplanung des Bundes muss ebenso beachtet werden wie architektonische oder Format-Vorgaben des SAGA-Standards. Zudem gilt es, die zunehmend verfügbaren Dienstleistungen der DLZ-IT zu berücksichtigen und ggf. in Anspruch zu nehmen. Die zu beachtenden strategischen Aspekte umfassen folglich

- die generelle SAGA-Konformität,
- die Beachtung der in SAGA genannten grundlegenden Kriterien wie Offenheit, Agilität und Wiederverwendbarkeit,
- die Herstellerunabhängigkeit und Stärkung des Wettbewerbs durch die Verwendung und Einführung offener Standards und Protokolle,
- die Harmonisierung der Software-Strategien der Bundesbehörden und die Vereinheitlichung der Standard-Softwarelandschaft in den Bundesbehörden,
- die Konzentration des internen Know-Hows auf Standard-Komponenten und deren Wiederverwendung,
- die Konzentration von externen Dienstleistungen auf wenige Standard-Komponenten,
- die Schaffung rechtlicher Klarheit, insbesondere bei bisher unkontrolliert eingesetzter OSS, sowie
- die dauerhafte Wirtschaftlichkeit über einen Zeitraum von sieben bis zehn Jahren.

Bei jeder Änderung des bestehenden Systems sollte daher geprüft werden, welche Teilsysteme und Komponenten auch künftig Teil der IT-Strategie sein oder ggf. zusammen mit dem eigentlichen Migrationsobjekt abgelöst werden sollen. Auch seit langem etablierte Bestandteile gehören immer wieder neu auf den Prüfstand, um die Auswirkungen deren Einsatzes auf das Gesamtsystem und deren Konformität zu strategischen Vorgaben zu beleuchten.

Mit diesen Überlegungen stehen der IT-Rat und die deutschen Bundesbehörden nicht alleine, wie das Beispiel der IT-Strategie der britischen Regierung zeigt. Diese will laut ihrem Cabinet Office bei den IT-Kosten sparen und sich zugunsten kleinerer, flexiblerer Projekte von Großinstallationen verabschieden (Cab11). In Zukunft soll mehr Open-Source-Software eingesetzt und eine zentrale Website der Verwaltung eingerichtet werden. Außerdem weist sie auf die Bedeutung von Interoperabilität durch die Verwendung offener Standards hin und regt das Teilen und Wiederverwenden von IT-Systemen und -Services im Public Sector an.

Der Migrationsleitfaden unterstützt den Prozess der Prüfung, der Beleuchtung von Alternativen und der Entscheidungsfindung, indem er die zu betrachtenden Aspekte prozessorientiert beschreibt, Bewertungskriterien aufstellt und daraus abgeleitete Empfehlungen ausspricht.

## 3.4 Rechtliche Aspekte

Jede Software-Migration muss die rechtlichen Aspekte des künftigen Teilsystems beleuchten. Je nach Art und Herkunft der künftigen Software ergeben sich beispielsweise Rechtsfragen in Bezug auf zugesicherte Eigenschaften, Gewährleistung, Verwendungsmöglichkeiten, Dienstleistungen wie Einrichtungs- und Betriebsunterstützung, Anzahl erlaubter Installationen oder Verwendung in virtualisierten Umgebungen. Zudem steht eine Migrationsentscheidung stets unter der Prämisse der vergaberechtlichen Zulässigkeit. Diese Fragen sind prinzipiell unabhängig von der mit der Software verbundenen Lizenz zu klären.

Beim Bezug proprietärer Software müssen alle regelungsbedürftigen Aspekte für deren Einsatz mit dem Hersteller oder Anbieter vertraglich vereinbart werden. Die Software darf ausschließlich im vertraglich vereinbarten Umfang genutzt werden, Art und Umfang der Ansprüche gegen den Vertragspartner sind vertraglich geregelt. Diese vertragliche Fixierung begründet eine gewisse Rechtssicherheit, die bei Open-Source-Software oft nicht vermutet wird.

Die Rechtsfragen, die sich beim Einsatz von OSS stellen, bieten bei näherer Betrachtung allerdings kein stichhaltiges Argument gegen die Verwendung durch Behörden. Die Vereinbarkeit des Lizenzmodells mit den relevanten Normen des Urheber-, Patent-, Haushalts- und Verwaltungsrechts wurde in den letzten Jahren mehrfach von deutschen Gerichten bestätigt. Auch hat der Gesetzgeber Bestimmungen in das Urheberrechtsgesetz aufgenommen, die zur rechtlichen Absicherung der GNU General Public License und der anderen OSS-Lizenzen beigetragen haben. Die Beherrschbarkeit der rechtlichen Risiken zeigt sich im Übrigen daran, dass in Deutschland keine Fälle bekannt geworden sind, bei denen Nutzer von OSS wegen Rechtsverstößen rechtlich belangt worden sind. Die rechtlichen Risiken sind in der Summe deswegen nicht gravierender als bei herkömmlich lizenzierten Programmen[6].

Aus der Sicht einer Behörde sind zwei Szenarien zu unterscheiden. In vielen Fällen haben Behörden keine über die reine Nutzung hinausgehenden Rechte an der in Frage stehenden OSS, weil sie diese weder geschrieben noch modifiziert haben. Die Behörde nutzt die Software dann als Lizenznehmer nach Maßgabe der jeweiligen OSS-Lizenz (hierzu sogleich unter 3.4.1). Hiervon zu unterscheiden ist der Fall, in dem die Behörde ein selbst entwickeltes Programm anderen Behörden oder Privaten als OSS zur Verfügung stellt bzw. ein vorbestehendes OSS-Programm in veränderter Form weitergeben möchte. In diesem Fall ergeben sich zusätzliche Rechtsfragen (hierzu unter 3.4.2).

### 3.4.1 Behörde als Nutzer und Lizenznehmer

Bei der Nutzung von OSS wird oftmals übersehen, dass für die bestimmungsgemäße Benutzung eines Programms nicht der Abschluss eines Lizenzvertrags erforderlich ist. Dies ergibt sich aus § 69d Abs. 1 UrhG. Sofern eine Behörde OSS auf einem Datenträger erwirbt oder aus dem Internet herunterlädt und das Programm lediglich benutzt, ohne es zu vervielfältigen, zu verbreiten, öffentlich zugänglich zu machen oder zu verändern, so ist der Abschluss eines OSS-Lizenzvertrags nicht erforderlich. Die Rechte und Pflichten der GNU General Public License oder anderer OSS-Lizenzen sind für die Behörde dann ohne Bedeutung. Erwirbt die Behörde das Programm in diesem Fall entgeltlich, etwa durch den Kauf einer kommerziellen Distribution, so bestehen gegen den Verkäufer die normalen Mängelgewährleistungs- und Haftungsansprüche. Hier ergeben sich keine Unterschiede zur Anschaffung proprietärer Software. Hat die Behörde die Software dagegen kostenlos erhalten, so bestehen Ansprüche auf Mängelgewährleistung nur, wenn die Mängel arglistig verschwiegen wurden. Auch haftet die Person, von der die Behörde das Programm erworben hat, für sonstige Schäden nur bei grober Fahrlässigkeit. Diese weniger weitreichende Haftung ergibt sich aus der Anwendung der Vorschriften zum Schenkungsvertrag, weil es sich um eine unentgeltliche Überlassung handelt.

[6] Siehe auch Unterlage für Ausschreibung und Bewertung von IT-Leistungen (UfAB V) Version 2.0, insbesondere 4.42 MODUL: Beschaffung von Open Source Software

Nur wenn die Behörde die Software vervielfältigt, verbreitet, verändert oder öffentlich zugänglich macht, bedarf sie der Rechte aus der betreffenden OSS-Lizenz. Erst bei dieser gesteigerten Nutzung kommt es also zum Abschluss eines Lizenzvertrags. Die üblichen OSS-Lizenzen gewähren der Behörde in diesem Fall weitreichende Nutzungsrechte. Allerdings beinhalten die OSS-Lizenzen auch mehr oder weniger weitreichende Pflichten, die die Behörde einzuhalten hat. Alle OSS-Lizenzen verpflichten den Lizenznehmer dazu, mit jeder Kopie des Programms auch eine Kopie des Lizenztexts mitzuliefern und die Hinweise auf die Geltung der Lizenz unverändert mitzuverbreiten. Typisch ist auch die Pflicht, einen Haftungs- und Gewährleistungsausschluss und die bestehenden Copyright-Vermerke unverändert mitzuverbreiten. Dagegen sehen nur einige OSS-Lizenzen die Pflicht vor, die Quelltexte des Programms zur Verfügung zu stellen. Dieses Grundgefüge der Rechte und Pflichten wurde von deutschen Gerichten am Beispiel der GNU General Public License Version 2 und der GNU Lesser General Public License Version 3 für wirksam erklärt. Behörden können sich also darauf verlassen, dass sie entsprechende Rechte aus den Lizenzen erwerben können. Der Lizenzvertrag kommt dabei formfrei durch die Inanspruchnahme der Rechte der Lizenz zustande, also beispielsweise durch die Veränderung eines Programms.

Wenn Behörden Software aktiv verbreiten oder öffentlich zugänglich machen, so gehen sie das rechtliche Risiko ein, wegen Verletzung von Urheber- oder Patentrechten in Anspruch genommen zu werden, wenn das betreffende Programm die Rechte Dritter verletzt. In Frage kommen in diesem Fall Schadensersatz- und Unterlassungsansprüche. Behörden können zudem zur Übernahme der Kosten einer Abmahnung durch den Rechtsinhaber verpflichtet sein. Behörden sollten deswegen gerade bei wenig verbreiteten, erst seit kurzem verfügbaren OSS-Programmen sorgfältig prüfen, ob geistige Eigentumsrechte Dritter entgegen stehen, bevor sie das Programm weitergeben.

Schließlich sollten Behörden bei der Beschaffung von OSS darauf achten, dass die Regeln des Vergaberechts eingehalten werden. Ausschreibungen müssen neutral erfolgen und sollten keine Formulierungen enthalten, durch die Anbieter proprietärer Software von vornherein ausgeschlossen werden. Bei der Forderung nach der Einhaltung offener Standards dürfte dies stets gegeben sein. Auch dürfen typische Eigenschaften von OSS, insbesondere die Verfügbarkeit der Quelltexte, die Unabhängigkeit von einzelnen Anbietern beim Support sowie die Möglichkeit des Rechtserwerbs, durchaus gefordert werden. Die genannten Kriterien sollten in der Ausschreibung transparent gemacht werden, damit sie bei der Vergabeentscheidung berücksichtigt werden können. Werden diese Grundsätze eingehalten, so ergeben sich keine vergaberechtlichen Probleme bei der Anschaffung von OSS.

### 3.4.2 Lizenzierung verwaltungseigener Software als OSS

Wenn die Behörde eigene Entwicklungen oder Fortentwicklungen vorbestehender OSS nach den Bestimmungen einer OSS-Lizenz anderen Behörden und Privaten zur Verfügung stellen will, ergeben sich andere rechtliche Fragestellungen. Die Behörde ist dann Lizenzgeber im Rahmen des OSS-Entwicklungsmodells.

Eine entsprechende Lizenzierung behördeneigener Software als OSS setzt zunächst voraus, dass die Behörde Inhaberin der ausschließlichen Nutzungsrechte an dem Programm ist. Wenn die in Frage stehenden Programme von Bediensteten des jeweiligen Verwaltungsträgers geschrieben wurden, so können die Rechte auch ohne Abschluss einer besonderen Vereinbarung gem. § 69b UrhG beim Arbeitgeber liegen. Der Erwerb ausschließlicher Rechte auf der Grundlage von § 69b UrhG ist jedoch an enge Voraussetzungen geknüpft. Die Rechtsprechung hat die Vorschrift in der Vergangenheit eher arbeitnehmerfreundlich ausgelegt. Der Rechtserwerb gem. § 69b UrhG muss deswegen im Einzelfall geprüft werden. Bei Entwicklungen durch externe Auftragnehmer bedarf es der ausdrücklichen Einräumung ausschließlicher Nutzungsrechte, damit die Behörde ein Programm als OSS lizenzieren kann. Zur Sicherheit sollte sowohl bei Bediensteten als auch bei externen Programmierern eine ausdrückliche Einwilligung in die Verwendung als OSS eingeholt werden.

Die Weitergabe von OSS an andere Behörden und Private ist des Weiteren an die haushaltsrechtlichen Vorgaben der §§ 61, 63 BHO bzw. an die entsprechenden landesrechtlichen Vorschriften gebunden. Eine Weitergabe und Lizenzierung von OSS an andere Behörden ist haushaltsrechtlich im Grundsatz

zulässig, da diese von den „Kieler Beschlüssen“ und den entsprechenden haushaltsrechtlichen Umsetzungsvorschriften im Bund und den Ländern gedeckt ist. Die „Kieler Beschlüsse“ decken aber nicht die Weitergabe an private Parteien. Bei Privatpersonen ist nur eine Weitergabe von Fortentwicklungen von Programmen zulässig, sofern diese einer Copyleft-Lizenz unterstehen. Im praktisch wichtigsten Fall, der Fortentwicklung von GPL-Software, darf die Behörde die eigenen Entwicklungsanteile ohne Erhebung von Lizenzgebühren an Private weitergeben. Bei vollständigen Neuentwicklungen und Fortentwicklungen von Non-Copyleft-Programmen ist die kostenlose Weitergabe an Private aber haushaltsrechtlich unzulässig.

Behörden müssen bei der Weitergabe und Lizenzierung von OSS schließlich auch die Vorgaben des Wettbewerbsrechts einhalten. Erstens dürfen Behörden gem. § 4 Nr. 1 UWG nicht ihre Autorität und das ihnen entgegengebrachte besondere Vertrauen der Bürger dazu nutzen, um von ihnen angebotene Waren oder Dienstleistungen im Markt zu platzieren; bspw. sollte der Datenschutzbeauftragte des Bundes ein Mailverschlüsselungsprogramm nicht als besonders sicher anpreisen, wenn er es selbst verbreitet. Zweitens kann die Weitergabe von OSS durch Behörden zu Verdrängungswettbewerb und dadurch zu einem Verstoß gegen § 3 UWG führen. Das Wettbewerbsrecht ist aber erst tangiert, wenn eine ernstliche Gefahr für den Bestand des Wettbewerbs auf einem spezifischen Markt besteht. Solange das Angebot der öffentlichen Hand mit marktstarken Konkurrenzprodukten im Wettbewerb steht, besteht diese Gefahr nicht und ergeben sich keine besonderen Pflichten für Behörden. Nur wenn eine Gefährdung des Wettbewerbs zu befürchten ist, müssen Behörden darauf achten, dass nicht durch den intensiven Einsatz öffentlicher Mittel weniger finanzstarke Mitbewerber aus dem Markt gedrängt werden.

Wenn Behörden Eigentwicklungen als OSS zur Verfügung stellen, so können sie die hierfür verwendeten Lizenzbestimmungen auswählen. Bei der Wahl der „richtigen“ Lizenzbestimmungen sollten verschiedene Aspekte sorgsam abgewogen werden: Erstens sollte die Rechtssicherheit bei den verschiedenen Lizenzmodellen bei der Entscheidung berücksichtigt werden. Zweitens sollte die Kombinierbarkeit des Programms mit anderen OSS-Komponenten beachtet werden. Drittens sollte beachtet werden, ob die Behörde für den Erfolg der (weiteren) Programmentwicklung auf die Mitarbeit bisher nicht beteiligter Entwickler setzt. Ist dies der Fall, so sollte eine Lizenz mit mindestens beschränktem Copyleft-Effekt ausgewählt werden, weil diese Lizenzen erfahrungsgemäß zu einem erhöhten Rückfluss von Entwicklerbeiträgen in die Gemeinschaft sorgen. Viertens sollte bei der Auswahl zwischen den Lizenzen beachtet werden, dass jede Entwicklergemeinschaft „ihre“ Lizenzbestimmungen bevorzugt. Wünscht man sich die Mitarbeit bestimmter Kreise, so ist die Verwendung der in diesen Entwicklerkreisen bevorzugten Lizenzbestimmungen Voraussetzung dafür, dass eine Beteiligung in nennenswertem Umfang stattfindet. Fünftens besteht die Möglichkeit, eigene Lizenztexte zu entwickeln. Die Verwendung eigener Lizenzbestimmungen eröffnet Behörden zusätzliche Gestaltungsspielräume, gestattet das Verfassen rechtlich abgesicherter Bestimmungen und erhält die Unabhängigkeit von der Lizenzierungspolitik anderer Organisationen, auf die in aller Regel kaum Einfluss genommen werden kann. Diese Option sollte allerdings nur bei der Freigabe abgeschlossener Programmentwicklungen in Betracht gezogen werden, weil sich die Mitarbeit externer Programmierer aus der OSS-Community hier signifikant verringern wird.

Steht nicht die Weitergabe einer vollständigen Eigenentwicklung, sondern einer Fortentwicklung vorbestehender OSS in Frage, so sind zusätzliche Gesichtspunkte zu beachten. Zunächst ist ein Strukturmerkmal aller gängigen OSS-Lizenzen, dass Lizenznehmer nicht zur Veröffentlichung und Verbreitung von Fortentwicklungen von Programmen verpflichtet sind. Die Pflicht zur Freigabe von Fortentwicklungen in Copyleft-Lizenzen greift erst in dem Moment ein, in dem sich der Lizenznehmer seinerseits dazu entschließt, die Fortentwicklungen zu verbreiten oder öffentlich zugänglich zu machen. Solange Fehlerbeseitigungen, Fortentwicklungen, Patches oder sonstige Hinzufügungen sowie Kombinationen von OSS und anderen Programmen nur innerhalb einer juristischen Person verwendet werden, müssen weder Nutzungsrechte eingeräumt noch Quelltexte der Programme an den ursprünglichen Lizenzgeber oder sonstige Dritte überlassen werden. Um eine nicht-öffentliche Nutzung handelt es sich auch dann, wenn eine größere Zahl von Vervielfältigungen hergestellt und innerhalb einer größeren juristischen Person des öffentlichen Rechts, etwa einer großen Kommune oder Bundesanstalt, weitergegeben wird. Gleiches gilt, wenn Kopien zwischen Behörden desselben Verwaltungsträgers ausgetauscht werden.

Ebenfalls um keine Weitergabe im urheberrechtlichen Sinn handelt es sich bei der Übergabe auftragsgemäß veränderter OSS vom Auftragnehmer an den Auftraggeber. Erst wenn das Programm an eine andere juristische Person, etwa eine andere Körperschaft des öffentlichen Rechts, eine andere Anstalt oder einen anderen Verwaltungsträger weitergegeben wird, handelt es sich um eine öffentliche Verbreitung mit der Folge, dass der Copyleft-Effekt der OSS-Lizenzen eingreift. Verbreitet die Behörde Fortentwicklungen von OSS oder Softwarekombinationen aus OSS und Eigenentwicklungen öffentlich, so ist bei OSS-Lizenzen mit Copyleft-Klausel zu prüfen, ob die Fortentwicklung oder Softwarekombination nach den Bestimmungen der für das OSS-Programm maßgeblichen Lizenz lizenziert werden muss. Der genaue Umfang dieser Verpflichtung ist in den OSS-Lizenzen sehr unterschiedlich geregelt und bedarf der Prüfung im Einzelfall.

Die angesprochenen Themen werden im Begleitdokument „Rechtliche Aspekte der Nutzung, Verbreitung und Weiterentwicklung von OSS“ zum Migrationsleitfaden[7] ausführlich diskutiert. Dort findet sich auch eine Aufstellung der verbreitetsten OSS-Lizenzen und im Anhang deren jeweiliger Wortlaut.

[7] http://www.cio.bund.de/mlf

## 3.5 Wirtschaftliche Aspekte

Gemäß §7 der Bundeshaushaltsordnung (BHO) gilt für die Aufstellung und Ausführung des Haushaltsplans der Grundsatz der Wirtschaftlichkeit. Daher müssen für alle finanzwirksamen Maßnahmen angemessene Wirtschaftlichkeitsuntersuchungen durchgeführt werden. Das WiBe-Fachkonzept[8] beschreibt ein insbesondere für IT-Maßnahmen geeignetes Vorgehen zur Bewertung der Wirtschaftlichkeit. Um die Besonderheiten einer Softwaremigration noch stärker zu berücksichtigen, wurde eine Vorhabensspezifische Anpassung des darin enthaltenen Kriterienkatalogs vorgenommen. Die so entstandene WiBe für Migrationen (Migrations-WiBe) steht als separates Begleitdokument des Migrationsleitfadens zur Verfügung[7] .

Das im WiBe-Fachkonzept definierte Vorgehen zur Bewertung der monetären und erweiterten Wirtschaftlichkeit bleibt dabei unverändert. Auf eine Beschreibung der anzuwendenden Verfahren (z.B. zur Berechnung des Kapitalwertes) wurde daher verzichtet. Die WiBe für Migrationen enthält neben einigen weiterführenden Hinweisen zur Durchführung einer Wirtschaftlichkeitsbetrachtung im Wesentlichen den überarbeiteten Kriterienkatalog.

Die Bewertung der Wirtschaftlichkeit einer Migrationsmaßnahme sollte demnach unter Verwendung des im WiBe-Fachkonzept beschriebenen Vorgehens und des vorhabenspezifischen Kriterienkatalogs erfolgen. Mit dem WiBe Kalkulator[9] steht eine an das WiBe-Fachkonzept ausgerichtete Software zur Durchführung von Wirtschaftlichkeitsbetrachtungen zur Verfügung. Die Software kann kostenfrei auf der Internetseite der IT-Beauftragten der Bundesregierung heruntergeladen werden[10].

Bei der Betrachtung der Wirtschaftlichkeit müssen alle migrationserheblichen Aspekte berücksichtigt werden. Sind neben der Software-Beschaffung weitere externe Leistungen wie Softwareanpassungen[11], Einrichtungsunterstützung oder Schulungen[12] notwendig und werden diese gem. § 97 (3) GWB in Lose aufgeteilt vergeben, darf dadurch insgesamt das Wirtschaftlichkeitsgebot nicht umgangen werden. Es muss also stets die Gesamtwirtschaftlichkeit einer Migration betrachtet werden.

[8] http://www.cio.bund.de/wibe

[9] Die zum Zeitpunkt der Erstellung dieses Dokuments verfügbare Version 1.0.1 des WiBe Kalkulators verwendet standardmäßig die im Migrationsleitfaden 3.0 enthaltene ältere Version des Kriterienkatalogs für Migrationsmaßnahmen.

[10] http://www.cio.bund.de/DE/Architekturen-und-Standards/Wirtschaftlichkeitsbetrachtungen/Software/software_node.html

[11] Siehe Migrations-WiBe Kriterium 1.1.2.2.2

[12] Siehe Migrations-WiBe Kriteriengruppe 1.1.3

## 3.6 Qualitative Aspekte

Neben der Wirtschaftlichkeit spielen bei der Migration auch qualitative Aspekte eine wichtige Rolle. Die migrierte Software darf, insbesondere aus Sicht der Anwender, nicht als Verschlechterung empfunden werden. Vor allem bestehende Eigenschaften, auch wenn diese nicht unmittelbar die Funktion der Software betreffen, sollten nach Möglichkeit erhalten bleiben. Andernfalls sinkt die wahrgenommene Qualität einer Software und somit die Akzeptanz der Anwender. Bei der Migration auf etablierte Industriestandards ist eine Untersuchung der qualitativen Aspekte in der Regel nicht notwendig. Aufgrund der hohen Akzeptanz und Verbreitung solcher Standards kann eine hinreichende Softwarequalität angenommen werden.

Für die Bestimmung der Softwarequalität existieren verschiedene Modelle und Methoden. Die ISO-Norm ISO/IEC 25010[13], ein international anerkannter Standard, definiert eine Reihe von Qualitätsmerkmalen zur Bewertung eines Softwareprodukts (Product quality model). Bei einer Migration empfiehlt es sich, diese als Basis für eine Prüfung zu verwenden. Welche Eigenschaften im konkreten Fall relevant sind, ist abhängig von der jeweiligen Migrationsmaßnahme und muss im Vorfeld individuell festgelegt werden. Die ISO-Norm gliedert die qualitative Bewertung eines Softwareprodukts in die nachstehend aufgeführten acht Bereiche[14]; die anschließenden Aspekte ab 3.6.9 sind zwar nicht in der ISO-Norm enthalten, sollten jedoch ebenfalls beachtet werden.

### 3.6.1 Funktionale Eignung

Die wichtigste Voraussetzung für den Einsatz einer Software ist die funktionale Eignung (*Functional Suitability*). Hierfür muss untersucht werden, ob die benötigte Funktionalität vollständig, korrekt und in geeigneter Weise durch die Software abgedeckt wird. Eine funktionale Eignung liegt vor, wenn die Software alle geforderten Funktionen fehlerfrei und ohne unnötige Zwischenschritte bereitstellt.

### 3.6.2 Leistungsfähigkeit

Sofern in den Anforderungen an die Software konkrete Leistungsparameter (Minima und/oder Maxima) benannt sind, ist zu prüfen, ob diese korrekt eingehalten werden (*Performance Efficiency*). Beispiele hierfür sind:

- Antwortzeiten
- Durchsatz
- Speicherbedarf
- Prozessorauslastung
- Bandbreite
- Anzahl paralleler Benutzer

Abhängig von den zu prüfenden Parametern empfiehlt es sich, die Messung mithilfe entsprechender Analysewerkzeuge durchzuführen. Um aussagekräftige Ergebnisse zu erzielen, sollte das zu prüfende System dabei unter (Voll-)Last arbeiten.

### 3.6.3 Kompatibilität

Für die Bewertung der Kompatibilität (*Compatibility*) muss untersucht werden, ob die Software parallel mit den ebenfalls auf dem System installierten Programmen betrieben werden kann. Neben einer feh-

[13] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35733
[14] Die englischen Original-Bezeichner der Bewertungsbereiche sind im jeweiligen Text als kursiv gedruckter Klammerzusatz enthalten.

lerhaften Ausführung können bei gleichzeitiger Nutzung von Hard- oder Software negative Seiteneffekte wie etwa eine Verschlechterung der Leistungsfähigkeit auftreten.

Die auch von SAGA geforderte Interoperabilität ist ein weiteres Kriterium zur Bestimmung der Kompatibilität. Hier ist zu prüfen, inwieweit die Software Daten für andere Systeme bereitstellen bzw. bereitgestellte Daten einlesen und auswerten kann.

### 3.6.4 Benutzbarkeit

Die Benutzbarkeit (*Usability*) einer Software lässt sich häufig nur subjektiv beurteilen. Die nachstehenden Eigenschaften sind Indikatoren einer guten Benutzbarkeit.

- Die bereitgestellte Funktionalität und die Eignung der Software lassen sich leicht erkennen.
- Die Bedienung der Software ist intuitiv und ohne großen Aufwand auch von fachfremdem Personal erlernbar.
- Die Software unterstützt den Benutzer bei der Vermeidung von Fehlern, beispielsweise durch die Kennzeichnung von Pflichtfeldern oder Wertebereichen.
- Die Benutzerschnittstelle der Software vermittelt ein ästhetisches Design (Farben, Schriftarten, Positionierung von Feldern usw.).
- Die Software kann von behinderten Menschen bedient werden.

Der zuletzt genannte Punkt bildet ein wesentliches Kriterium bei der Überprüfung der Benutzbarkeit: Eine SAGA-konforme Software muss die gemäß BITV[15] an die Barrierefreiheit gestellten Anforderungen erfüllen.

### 3.6.5 Zuverlässigkeit

Die Zuverlässigkeit (*Reliability*) des Gesamtsystems wird in erster Linie durch die verwendete Hardware und die Verfügbarkeit des Netzwerkes bestimmt. Mithilfe redundanter Systeme sowie mit Verfahren zur Lastverteilung kann die Ausfallsicherheit und damit die Zuverlässigkeit des Gesamtsystems zusätzlich gesteigert werden. Um die Zuverlässigkeit der Software zu beurteilen, muss deren Fehlertoleranz (Verhalten bei Hardware- oder Softwarefehlern) analysiert werden. Hierzu zählen beispielsweise die zum automatischen Zwischenspeichern oder für eine Datenrückgewinnung angebotenen Funktionen. Der Einsatz erprobter Laufzeitumgebungen ist ebenfalls ein wichtiges Kriterien für die Bewertung der Zuverlässigkeit.

### 3.6.6 Sicherheit

Entscheidend für die Sicherheit (*Security*) einer Software ist die vorhandene Netzwerksicherheit, d.h. die zum Schutz des Netzwerkes getroffenen Maßnahmen. Diese sind detailliert in den IT-Grundschutz-Katalogen[16] beschrieben. Die Software selbst sollte Mechanismen (beispielsweise eine Benutzerverwaltung) bereitstellen, um einen unautorisierten Datenzugriff zu verhindern. Die nicht manipulierbare Protokollierung durchgeführter Aktionen, das sogenannte Logging, bildet ebenfalls ein wichtiges Sicherheitsmerkmal.

### 3.6.7 Wartbarkeit

Die Wartbarkeit (*Maintainability*) gibt Auskunft darüber, mit welchem Aufwand Korrekturen und Erweiterungen an einer Software möglich sind. Hier ist zu prüfen, ob die Software modular aufgebaut ist und

[15] Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz: http://bundesrecht.juris.de/bitv/

[16] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

damit einzelne Module unabhängig voneinander angepasst werden können. Sind die Auswirkungen einer Änderung sowie die Ursache eines Fehlers leicht zu analysieren, spricht dies ebenfalls für eine gute Wartbarkeit.

### 3.6.8 Portabilität

Als entscheidendes Kriterium für die Bewertung der Portabilität (*Portability*) muss die Plattformunabhängigkeit der Software untersucht werden. Neben dem Betriebssystem ist auch die Verwendung unterschiedlicher Laufzeitumgebungen (z.B. Java Application Server) und/oder Datenbanken zu prüfen. Dabei muss der zur Installation, Deinstallation und zum Update der Software benötigte Aufwand berücksichtigt werden.

### 3.6.9 Dokumentationsgüte

Nicht in der ISO/IEC 25010 enthalten sind Aussagen zur Dokumentationsgüte, die allerdings für die Bewertung eines Software-Produkts durchaus relevant sind. Für die migrierte Software werden je nach Art der Migration verschiedene Dokumentationen benötigt. SAGA beschreibt als Mindestanforderung an die Offenheit eine kostenfreie oder gegen ein angemessenes Entgelt erhältliche Dokumentation (siehe Abschnitt 2.2 auf Seite 9). Das V-Modell XT Bund[17] definiert darüber hinaus bereits Prüfkriterien zur Absicherung der Dokumentationsgüte einer Software[18]. Diese gelten ohne Einschränkungen auch für die Migration und umfassen

- eine Dokumentation des Funktionsumfangs,
- eine Installationsanleitung,
- eine Schnittstellenbeschreibung,
- Verwendungsbeispiele,
- eine Dokumentation der Erweiterungsmöglichkeiten,
- eine Konfigurationsanleitung sowie
- ein Benutzerhandbuch.

Bei der Prüfung ist gemäß V-Modell XT Bund, abhängig vom jeweiligen Typ der Dokumentation, auf eine akzeptable Qualität zu achten bezüglich

- der Gliederung,
- der Übersichtlichkeit,
- der Navigierbarkeit,
- konsistenter und korrekter Terminologie,
- der Vollständigkeit,
- der Verständlichkeit und
- des sprachlichen Ausdrucks.

Die den Anwendern bereitgestellten Dokumentationen müssen in deutscher Sprache vorliegen.

### 3.6.10 Konfigurierbarkeit

Ein weiteres Qualitätsmerkmal, insbesondere für Multi-User-Anwendungen, besteht in der Konfigurierbarkeit der Software. Hier ist zu prüfen, ob und in welchem Umfang es die Software ermöglicht, den

[17] http://www.bit.bund.de/cln_180/nn_1202296/BIT/DE/Standards__Methoden/V-Modell_20XT/node.html?__nnn=true

[18] Die im V-Modell XT enthaltenen Prüfkriterien beziehen sich auf die Evaluierung von Fertigprodukten, d.h. auf die bei einer Marktsichtung potentieller Software(-Bausteine) zu prüfenden Eigenschaften.

Benutzern verschiedene Rechte und Rollen zuzuweisen und die Software für rollenspezifisches Verhalten zu konfigurieren.

Im Rahmen der Konfigurierbarkeit kann zudem untersucht werden, ob die Benutzer eigene Einstellungen (z.B. Farben oder Schriftarten) vornehmen und diese benutzerspezifisch speichern können. Solche Eigenschaften, auch wenn diese die Funktion der Software nicht unmittelbar betreffen, erhöhen maßgeblich die Akzeptanz.

### 3.6.11 Sonstige Qualitätsmerkmale

Neben der Dokumentationsgüte enthält das V-Modell XT Bund weitere Prüfkriterien für die Qualitätsbewertung einer Software, die bei Bedarf zur Entscheidungsfindung herangezogen werden sollten. Dies sind

- Firmengröße und -bestehen des Softwareherstellers oder Aktivität der Community,
- Anzahl und durchschnittliche Dauer zur Behebung bekannter Fehler,
- Art und Umfang des bereitgestellten Supports (Herstellersupport, Internetforen, Newsgroups) sowie
- die Qualität des Quellcodes.

Eine Analyse des Quellcodes ist typischerweise nur bei Open-Source-Software möglich und aufgrund des verhältnismäßig hohen Aufwands auch nur in Ausnahmefällen sinnvoll, beispielsweise wenn für die Software infolge geringer Verbreitung keine hinreichende Aussage über die vermutliche Qualität getroffen werden kann. Zur automatisierten Quellcodeanalyse stehen verschiedene kostenfrei erhältliche Werkzeuge zur Verfügung[19].

[19] Siehe beispielsweise http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis

## 3.7 Aspekte des Systembetriebs

### 3.7.1 Weitere Arten der Migration aus Sicht des Systembetriebs

In Kapitel 2.1 sind Migrationen unter dem Aspekt der Veränderung der bereitgestellten Anwendungen oder Produkte betrachtet worden. Dieses zielt auf die für den Anwender sichtbaren Bereiche der Migration. Unter den Gesichtspunkten des Systembetriebes gibt es weitere Arten der Migration, die im Idealfall vom Anwender nicht wahrgenommen werden, für den Systembetrieb jedoch auch eine Migrationsherausforderung darstellen und in diesem Kapitel benannt werden.

Die für den Systembetrieb eingesetzte Hardware unterliegt einem Alterungsprozess, die die notwendige Verfügbarkeit der Anwendungen gefährden kann oder nach heutigem Stand der Technik unwirtschaftlich oder auch energieineffizient ist. In solchen Fällen wird häufig eine technische Migration durchgeführt, bei der die eingesetzten Hardwareressourcen ausgetauscht werden, die Anwendung jedoch unverändert weiterbetrieben wird.

Ein deutlich weitergehender Schritt ist die Verlagerung des Anwendungsbetriebes vom derzeitigen Standort an einen anderen. Wird die betriebene Hardware nur von einem Rechnerraum oder Rechenzentrum in ein anderes verlagert und anschließend weiterhin vom bisherigen Betriebsteam betreut, handelt es sich um einen Umzug der Anwendung. Gründe für die Verlagerung von Rechnerräumen können beispielsweise Engpässe in der Gebäudeinfrastruktur oder Standortverlagerungen sein.

Wenn die Betriebsverantwortung für eine Applikation von dem bisherigen Team auf ein neues Team oder einen externen Dienstleister übergeht, dann wird das Sourcingmodell für die Anwendung geändert. Häufig wird der Anwendungsbetrieb ausgelagert, um über den Betrieb bei einem spezialisierten Dienstleister Skaleneffekte zu nutzen und eigene Personal- und Managementkapazitäten statt für den IT-Betrieb für die eigentlichen Kernaufgaben einzusetzen.

### 3.7.2 Service Level Agreements (SLAs)

Unter dem Namen IT Infrastructure Library (ITIL) hat sich eine Sammlung von Praktiken für den IT-Systembetrieb als de-facto-Standard entwickelt. Um für die zu migrierende Anwendung eine angemessene Systeminfrastruktur bereitstellen zu können, müssen die Anforderungen an die Anwendung gemäß ITIL als SLA beschrieben werden. SLAs haben je nach Einsatzgebiet und Anwendung einen unterschiedlich großen Umfang. Als Mindestanforderung sind in den SLAs die folgenden Anforderungen zu vereinbaren:

- Verfügbarkeit der Anwendung
- Maximale Ausfallzeit der Anwendung
- Maximal tolerierbare Zeitspanne des Datenverlustes
- Betriebszeiten der Anwendung
- Mengengerüste der Anwendung (z.B. Anzahl gleichzeitiger Nutzer, Datenvolumina)
- Wenn benötigt Performancekennzahlen (Antwortzeiten)
- Klärung, ob und in welchem Zeitrahmen der Betrieb in einem Ausweichrechenzentrum kurzfristig fortgeführt werden muss, falls der Standort, an dem die Anwendung betrieben wird, durch eine Katastrophe ausfällt (Desaster Recovery Anforderungen)

Das Bereitstellen einer angemessenen Infrastruktur bedeutet, dass diese darauf ausgelegt ist, die Service Level sicher zu erfüllen, ohne dabei wesentlich überdimensioniert zu sein, da dieses der Wirtschaftlichkeit entgegenlaufen würde.

Die in 3.9 betrachteten Kriterien für Sicherheitsaspekte fließen ebenfalls in die Anforderungen an den Systembetrieb ein, da das notwendige Schutzniveau beim Systemdesign zu berücksichtigen ist. Ins-

besondere auf die Fragen von dedizierten oder gemeinsam genutzten Infrastrukturkomponenten hat dieses einen Einfluss.

### 3.7.3 Anforderung an das Migrationsvorgehen

Ergänzend zum in den SLAs definierten Verhalten der Systeminfrastruktur im zukünftigen Betrieb müssen die Anforderungen an das Migrationsvorgehen definiert werden. Wesentliche zu klärende Fragen sind:

- Ist ein Parallelbetrieb von alter und neuer Anwendung möglich / gewünscht / notwendig?
- Wie lang ist die maximale Betriebsunterbrechung für die Migration und in welchen Zeitfenstern kann diese erfolgen?
- Werden die Daten von der alten Plattform vollständig migriert oder ist auch nach Abschluss der Migration ein Zugriff auf das Altsystem erforderlich?
- Werden für die Migration temporär zusätzliche Systeme benötigt?
- Welche Anforderungen gibt es bezüglich der Bereitstellung von Testumgebungen und Testdaten?

### 3.7.4 Auswahl der Infrastruktur und der Anwendungsprodukte

Durch die Standardisierung der eingesetzten Infrastrukturkomponenten ist es möglich, die Breite des vorzuhaltenden Wissens zu verringern und die Zahl der Lieferanten und Wartungsgeber zu begrenzen. Insbesondere bei Systemen mit hohen Verfügbarkeitsanforderungen ist der Systembetrieb darauf angewiesen, jederzeit Mitarbeiter mit entsprechenden Qualifikationen bereitzuhalten. Je heterogener die betriebene technische Infrastruktur ist, desto schwieriger, aufwendiger und teurer ist dieses.

Standardisierung beginnt bei eingesetzten Hardwarekomponenten wie Servern und Speichersystemen, geht über Betriebssysteme und Middleware-Komponenten wie Applikationsserver und Datenbanken bis hin zu Anwendungssystemen. Die bereits etablierten Forderungen zur Auswahl von herstellerunabhängiger Anwendungssoftware sollten dem Systembetrieb bei der Migration auf aktuelle Anwendungen die notwendigen Freiheitsgrade geben.

Diese Freiheitsgrade sind bei der ablösenden Migration dahingehend zu nutzen, dass die benötigten Eigenschaften und die zu erbringenden Leistungen funktional vollständig definiert werden, ohne dabei auf bestimmte Produkte oder Hersteller einzugehen. Lediglich die Anforderungen aufgrund gegebener Schnittstellen zu anderen Teilsystemen dürfen davon abweichen.

Bei der fortführenden Migration von Bestandsanwendungen sind diese Freiheitsgrade nur eingeschränkt vorhanden; Produkt- oder Herstellervorgaben können sachlich gerechtfertigt sein. Allerdings können über eine Analyse der kritischen Infrastrukturkomponenten aus den Bestandsanwendungen wichtige Anforderungen an die mittelfristig zu unterstützende Technologie gewonnen werden, die dabei helfen, die individuellen Schwerpunkte zu definieren und diese bei neuen Migrationen zu berücksichtigen.

Bei der Produktauswahl gibt es zwei Extrempositionen. Bei der einen geben die bereits in der IT-Landschaft vorhandenen Komponenten und Techniken vor, welche technischen Anforderungen an eine neue Applikation gestellt werden. Dies kann dazu führen, dass fachlich gut geeignete Anwendungen und Lösungen mangels Kompatibilität zur vorhandenen IT-Landschaft ausgeschlossen werden. Im anderen Fall wird die Lösung ausschließlich aufgrund der fachlichen Anforderungen ausgewählt und der Systembetrieb muss anschließend die unterstützende Infrastruktur implementieren und betreiben. Bei diesem Ansatz besteht die Gefahr, dass eine sehr heterogene Infrastruktur und Systemumgebung entsteht, die nur schwer zu beherrschen ist und hohe Betriebskosten erzeugt.

Der ITIL-Prozess *Service Catalog Management* hilft dabei, die Interessenkonflikte zwischen den beiden Ansätzen auszubalancieren und eine kontrollierte Service- und Infrastrukturentwicklung sicherzustellen. Dieser Prozess sollte bei Migrationen genutzt werden.

Ein weiterer Aspekt bei der Auswahl von Diensten und Infrastruktur-Komponenten ist der zu erwartende Resourcenbedarf. Angesichts steigender Anforderungen an die Energieeffizienz von Rechenzentren[20] unter dem Stichwort *Green IT*[21], aber auch von Desktop-Systemen sollten die Alternativen dahingehend bewertet werden, wie hoch deren Resourcenverbrauch hinsichtlich CPU-Last und Hauptspeicherverbrauch beim durchschnittlichen Einsatz anzusetzen ist. Hierzu sind die Angaben der Hersteller, unabhängige Tests Dritter und ggf. eigene Testergebnisse auszuwerten.

Mit der Virtualisierung von Diensten und Desktops kann ein höherer Auslastungsgrad von physikalischen Systemen erreicht und damit die Energieeffizienz gesteigert werden (siehe Abschnitt 4.2.5). In die Bewertung der Produkte sollte daher auch einfließen, ob die einzelnen Alternativen virtualisiert werden können und welche Voraussetzungen ggf. dazu notwendig sind. Diese Aspekte sollten auch bei der Wirtschaftlichkeitsbetrachtung (siehe Unterkapitel 3.5) berücksichtigt werden.

Zukünftig wird die Energieeffizienz von IT-Systemen und Anwendungen darüber hinaus danach beurteilt werden, welcher Energieeinsatz für die Erledigung eines Geschäftsprozesses oder Fachverfahrens benötigt wird. Insbesondere bei Auftrags- und Eigenentwicklungen sollte man daher die für Anwendungen verwendeten Middlewarekomponenten und Algorithmen auf ihre Effizienz untersuchen. Der Systembetrieb sollte in diese Untersuchungen eingebunden werden und in der Evaluationsphase gemeinsam mit den Fachbereichen eine Bewertung vornehmen.

### 3.7.5 Wartungsverträge und Lizenzmodelle

Neben den einmaligen Investitionskosten sind die externen laufenden Kosten für den Betrieb zu berücksichtigen und zu bewerten.

Für kritische Hardwareressourcen werden in der Regel Wartungs- und Supportverträge abgeschlossen, die sicherstellen sollen, dass Systeme im Fall von Störungen innerhalb der im SLA zugesagten Zeiten wiederhergestellt werden können. Da Hardware altert und Ersatzteile von den Herstellern nicht unbegrenzt lange zu den ursprünglichen Konditionen vorgehalten werden, steigen im Anschluss an die Garantie- oder Erstwartungslaufzeit die Wartungskosten im Regelfall an. Für die geplante Standzeit der Systeme sind diese Kosten im Rahmen der Wirtschaftlichkeitsbetrachtung zu berücksichtigen.

Für kritische Softwarekomponenten werden in der Regel ebenfalls Supportverträge abgeschlossen. Selbst bei Software, bei der aufgrund des Lizenzmodells keine Lizenzkosten anfallen, sollten Supportverträge mit Dienstleistern abgeschlossen werden, da im Regelfall intern kein Experten-Know-how vorhanden und im Störungsfall in definierten Zeiten ein Zugriff auf Expertenunterstützung notwendig ist. Die Supportverträge sollten so gestaltet sein, dass die Support- und Reaktionszeiten den Anforderungen der SLAs gerecht werden.

Da bei der Systemauswahl das Lastverhalten der Anwendung und die zukünftige Entwicklung der Nutzung nicht immer vorab bestimmt werden können, muss untersucht werden, wie die Anwendung im Bedarfsfall skaliert werden kann. Skalierungsvarianten müssen hinsichtlich der Lizenzmodelle und Lizenzierungskosten untersucht werden. Eine Skalierung führt im Regelfall auch zu veränderten Kosten von Wartungsverträgen.

Wartungsverträge und Lizenzmodelle sollten die zu erwartende Skalierung zu angemessenen Kosten zulassen.

### 3.7.6 Auswahl des Systembetreibers

Bei jeder größeren Migration muss der Betreiber der zukünftigen Infrastruktur ausgewählt werden. Diese Auswahl folgt der jeweiligen Sourcing-Strategie.

Grundsätzlich wird zwischen Eigenbetrieb und Fremdbetrieb unterschieden.

[20] Eine Kennzahl zur Bestimmung der Energieeffizienz ist beispielsweise die Power Usage Effectiveness (PUE).
[21] Siehe http://www.cio.bund.de/green-it

Beim Eigenbetrieb liegt die Betriebsverantwortung für den Systembetrieb im eigenen Haus. Der Auftraggeber und Anwendungsbetreiber hat direkten Einfluss auf die Steuerung des Systembetriebs. Er ist auf der anderen Seite jedoch auch technisch für diesen voll verantwortlich. Insbesondere bei kleinen Einheiten ist es schwierig, die baulichen, infrastrukturellen und personellen Voraussetzungen zu schaffen, um kritische IT-Systeme in einer angemessenen Umgebung zu betreiben.

Die Alternative dazu ist der Fremdbetrieb in Form von Outsourcing oder Outtasking. Hier werden einem Dienstleister definierte Aufgaben übertragen. In der Vorbereitungsphase der Migration wird hierbei festgelegt, welche Leistungen an einen externen Dienstleister vergeben werden sollen und für welche Leistungsbereiche die Verantwortung im eigenen Haus verbleibt. Werden größere Leistungsblöcke wie beispielsweise die Gesamtbereitstellung und der Betrieb einer Anwendung an einen Dienstleister vergeben, spricht man von Outsourcing. Werden nur einzelne kleinere Aufgaben (Tasks) an Dienstleister vergeben, spricht man von Outtasking.

Als externe Dienstleister werden alle Einheiten betrachtet, die außerhalb des eigenen Kontrollbereiches sind. Dies können IT-Töchter, die DLZ-IT, Zweckverbände oder am Markt agierende IT-Dienstleister sein.

Bei der Auswahl eines externen Dienstleisters sind neben den wirtschaftlichen Kriterien folgende Aspekte zu berücksichtigen:

- Verfügt der Dienstleister über die Kompetenzen, Erfahrungen und Ressourcen, um die geforderten SLAs sicher zu erfüllen?
- Ist der Dienstleister wirtschaftlich so stabil, dass er die Leistungen dauerhaft, mindestens jedoch über den Beauftragungszeitraum hinweg erfüllen kann?
- Ist der Dienstleister in der Lage, die Anforderungen der IT-Sicherheit zu erfüllen?
- Können durch den Betrieb der Anwendung beim Dienstleister Interessenkonflikte entstehen?

Bereits bei Abschluss des Vertrages mit dem externen Dienstleister sollte geregelt werden, dass dieser die kontrollierte Überführung der betriebenen Services an den Auftraggeber oder einen anderen Dienstleister unterstützt. Für den Fall einer Übernahme des Dienstleisters durch einen anderen Eigentümer, sollte ein außerordentliches Kündigungsrecht vereinbart werden.

Während im Eigenbetrieb die Organisation des IT-Betriebs nach ITIL *best practices* wünschenswert ist, sollte beim Fremdbetrieb eine ITIL-gemäße Organisation und Vertragsgestaltung vereinbart werden, um von den dort klar definierten Prozessen und Verantwortlichkeiten zu profitieren. Dabei ist nicht nur der Dienstleister hierauf festzulegen, sondern gleichzeitig sicherzustellen, dass im eigenen Haus das für das *Demand Management*[22] notwendige Fach- und Prozesswissen vorhanden ist.

Soll die Gesamtverantwortung für den Systembetrieb im eigenen Haus verbleiben, obwohl hier nicht alle notwendigen Kompetenzen oder Ressourcen verfügbar sind, so können diese Engpässe und Defizite über selektives Outtasking gelöst werden, bei dem einzelne Aufgaben bedarfsgerecht an einen spezialisierten Dienstleister übertragen werden. Liegen die Restriktionen im Bereich der Serverraum- oder Rechenzentrumsinfrastruktur, so besteht die Option der physikalischen Auslagerung der IT-Infrastruktur in ein externes Rechenzentrum (Housing).

Die partielle Auslagerung stellt genauso wie die Auslagerung von Systembetriebsleistungen an mehr als einen Dienstleister aufgrund der Vielzahl an Schnittstellen deutlich höhere Anforderungen an die Dienstleistungssteuerung im eigenen Haus und sollte nur dann erfolgen, wenn ausreichende Kenntnisse im Demand Management in der Organisation vorhanden ist.

[22] Steuerung und Kontrolle der beauftragten Dienstleister

## 3.8 Organisatorische Aspekte

Je größer die Außenwirkung einer Migration ist, das heißt, je mehr Veränderungen sich für die Anwender und die Behörde ergeben, desto umfassender sind die organisatorischen Aspekte einer Migration zu beachten.

In den Fällen, in denen sich außer einer möglichen Betriebsunterbrechung für den Anwender nichts Nennenswertes verändert, können die organisatorischen Aspekte auf die in den Abschnitten 3.8.1 bis 3.8.4 beschriebenen Kriterien beschränkt werden. Erfolgen im Rahmen einer Migration durch die Auswahl des IT-Systembetreibers Änderungen in der leistungserbringenden Einheit, ist Abschnitt 3.8.5 von Relevanz. Bei großen Migrationen mit deutlichen Auswirkungen auf die Anwender und beträchtlichen Veränderungen für den IT-Betrieb sind alle Kriterien dieses Abschnittes zu beachten.

### 3.8.1 Change Management

Der ITIL-Prozess *Change Management* stellt sicher, dass eine technische Migration auf eine kontrollierte Art und Weise erfolgt. Durch den Einsatz des Change Management-Prozesses werden technische Veränderungen (Changes) umgesetzt. Auslöser für diese Veränderungen können aus der Betriebsführung in Reaktion auf Probleme und Störungen und aus geänderten Anforderungen heraus gestellt werden. Ein wesentliches Ziel des Change Management Prozesses ist es, in Reaktion auf geänderte Anforderungen, unzureichende Stabilität, ungenügende Funktionalität oder geänderte Rahmenbedingungen den Nutzen der IT-Anwendung zu maximieren und gleichzeitig Unterbrechungen und Nacharbeiten zu reduzieren.

Die Veränderungsanforderungen werden als Requests for Change (RfCs) definiert und in den Change Management Prozess eingesteuert. Jeder Change dient dazu, die IT Services mit den Anforderungen des Auftraggebers in Übereinstimmung zu bringen. Damit unterstützen die Ziele des Change Management das Ziel einer erfolgreichen Migration.

Eine Migration oder auch wesentliche Einzelaktivitäten innerhalb der Migration werden per RfC als Change initiiert und dabei

- evaluiert,
- autorisiert,
- priorisiert,
- geplant,
- getestet,
- implementiert,
- dokumentiert und
- bewertet.

Durch dieses Vorgehen ist unter anderem sichergestellt, dass vor der Migration Test- und Abnahmeverfahren definiert und dokumentiert sind und dass sogenannte Fallback-Pläne existieren, die bei Problemen während der Migration sicherstellen, dass ein dokumentierter Plan existiert, der den kontrollierten Abbruch der Migration und eine Rückkehr zum Zustand vor Beginn der Migration ermöglicht.

Die Anforderungen, die das Change Management an das Vorgehen und die Projektrollen innerhalb von Projekten stellt, sind im V-Modell XT Bund berücksichtigt[23].

[23] V-Modell XT Bund, Version 1.0 — Teil 4 Abs. 2.3.7; IT Service Transition Verantwortlicher im Teilbereich Change Manager

### 3.8.2 Release Management

Das Release Management dient zur Planung, Überwachung und Durchführung von Release-Rollouts über die Testumgebung in die Live-Umgebung. Insbesondere stellt es sicher, dass die Integrität der Produktions-Umgebung geschützt wird und dass nur zuvor geprüfte Komponenten ausgerollt werden. Der Release Management und der Change Management Prozess arbeiten dabei sehr eng zusammen.

Durch Migrationen können Nebenwirkungen auf andere IT-Systeme und die Arbeitsplätze der Anwender ausgelöst werden. Das Release Management hilft hier durch Planung und Tests vorab sicherzustellen, dass diese Nebenwirkungen frühzeitig identifiziert und adressiert werden.

Insbesondere auf den Endgeräten der Anwender, auf denen viele unabhängige Anwendungen betrieben werden, kann es zu Problemen bei den Anforderungen an die Konfiguration der Endgeräte kommen. So existieren in vielen Fällen alte Softwarepakete, die nicht oder nicht ohne weiteres auf den aktuellen Hardware- und Betriebssystemplattformen laufen. Aktuelle Anwendungen benötigen jedoch häufig den aktuellen Stand der Technik und sind auf den alten Plattformen nicht einsetzbar.

Über das Release Management wird eine Gesamtplattform definiert und bereitgestellt, die die unterschiedlichen Anforderungen gemeinsam betrachtet und dabei über den Rand des einzelnen Migrationsprojektes hinaus schaut. Insbesondere das Zusammenspiel von Arbeitsplätzen und Backendsystemen wird sichergestellt.

Aus dem vor der Migration in Produktion befindlichem Release und den Änderungsanforderungen der Migration an das Release kann identifiziert werden, welche Veränderungen für die Migration notwendig sind.

Aus dem Release Management kann für Testumgebungen eine definierte Referenzplattform implementiert werden, die Integrationstests in Release-Ständen ermöglicht, die der zukünftigen Produktionsumgebung nach der Migration entsprechen. Durch Tests in dieser Umgebung kann im Vorfeld sichergestellt werden, dass nach der Migration im Feld keine unerwarteten technischen Probleme entstehen.

Werden Schnittstellen zu Systemen verändert, die sich außerhalb des Kernbereiches der jeweiligen Migration befinden, so kann ein Zielrelease definiert und implementiert werden, welches auf die Verträglichkeit mit der Bestandumgebung getestet werden kann. Hierdurch lassen sich negative Auswirkungen der Migration auf Drittsysteme weitestgehend vermeiden oder zumindest im Vorfeld identifizieren.

### 3.8.3 Zeitplanung

Eine Migration muss immer in den Gesamtkontext aller betriebenen IT-Systeme und der parallel laufenden IT-Projekte gestellt werden und kann nicht als isoliertes Projekt betrachtet werden.

Eine Grundvoraussetzung für eine Migration ist der Abschluss zuvor notwendiger Implementierungsarbeiten. Geschäftliche oder gesetzliche Anforderungen sowie parallel laufende Projekte oder Ressourcenengpässe können einerseits den Endetermin einer Migration vorgeben, andererseits aber auch der Grund für Verzögerungen sein, da die Migration zum ursprünglich geplanten Zeitpunkt nicht umgesetzt werden kann oder soll.

In einem vollumfänglich gelebten Change Management Prozess werden Konfliktsituationen und Terminkollisionen bereits dort identifiziert und aufgelöst. Aufgrund der Bedeutung einer guten Planung sollen die wesentlichen Kriterien hier jedoch eigenständig aufgeführt werden:

- Gibt es Sperrzeiten (Frozen Zones), in denen grundsätzlich keine Changes durchgeführt werden dürfen, um die Stabilität der Landschaft nicht zu gefährden?
- Werden parallel andere Changes durchgeführt, so dass es zu Ressourcenkonflikten bei den für die Umsetzung des Changes erforderlichen Mitarbeitern kommen kann?
- Besteht durch parallel durchgeführte Changes die Gefahr, so umfassende Veränderungen durchzuführen, dass im Fehlerfall eine kausale Analyse der Ursachen nicht mehr möglich oder ein Rollback des Gesamtsystems gefährdet ist?

- Stehen genügend Anwender in der geplanten Zeit für Tests zur Verfügung?
- Sind die Anwender ausreichend geschult?
- Können die Anwender ihren dienstlichen Verpflichtungen auch während der Mehrbelastung durch die Umstellung nachkommen?

### 3.8.4 Risikomanagement

Ziel des Risikomanagements ist es, Risiken zu identifizieren und zu bewerten, um sie dann je nach Bewertung zu vermeiden, zu vermindern oder zu tolerieren. Das Risikomanagement soll sicherstellen, dass keine unvorhergesehenen Risiken eintreten können. Das Risikomanagement innerhalb eines Migrationsprojektes ist der für diese Migration relevante Ausschnitt des ganzheitlich betriebenen IT-Risikomanagements.

Die im folgende aufgeführten Problemfelder helfen dabei, wesentliche mögliche Risiken bei Migrationsprojekten zu identifizieren:

- Akzeptanzprobleme aufgrund von Veränderungen in Abläufen und Geschäftsprozessen bei Anwendern, Auftraggebern oder der Öffentlichkeit,
- Akzeptanzprobleme aufgrund von Veränderungen in Verantwortung, Prozessen oder Technologien bei den für den Betrieb der Anwendung verantwortlichen Mitarbeitern,
- Technologieprobleme durch den Einsatz von noch nicht ausgereiften Komponenten oder von Technologien, die durch den Betreiber noch nicht beherrscht werden,
- Zeitprobleme aufgrund von Verzögerungen bei der Implementierung der Anwendung oder der Bereitstellung von Infrastrukturkomponenten,
- Budgetprobleme aufgrund falscher Einschätzung von Aufwand und Komplexität der Migration,
- Akzeptanzprobleme durch eine unzureichende Abdeckung der praktischen oder fachlichen Anforderungen durch die neue Lösung,
- Akzeptanzprobleme durch eine unzureichende Vorbereitung der Anwender auf den Einsatz der neuen Lösung,
- Technologieprobleme durch unvorhergesehene Wechselwirkungen mit anderen Anwendungen oder Komponenten der IT-Infrastruktur sowie
- Probleme innerhalb der Migrationsphase, die aus der Übernahme von Bestandsdaten oder dem Parallelbetrieb von alter und neuer Anwendung entstehen können.

Die im Risikomanagement identifizierten Risiken sind in den Zeitplänen, dem die Migration begleitenden Veränderungsmanagement und bei der Einbindung der von der Migration betroffenen Personen sowie den an der Migration beteiligten oder interessierten Personen und Gremien zu berücksichtigen. Die Gesamtheit der betroffenen, beteiligten und interessierten Personen und Gremien wird als *Stakeholder* bezeichnet.

### 3.8.5 Veränderungsmanagement innerhalb der IT

Durch Migrationen können innerhalb der für den Anwendungsbetrieb verantwortlichen IT Einheiten unterschiedliche Veränderungen entstehen:

- Neue Technologien, für die derzeit noch kein ausreichendes Wissen vorhanden ist,
- veränderte Betriebsprozesse und Verantwortlichkeiten,
- Wegfall von bisherigen Aufgaben und darauf basierenden Kompetenzgebieten,
- neue Aufgaben und Organisationsstrukturen,

- Ersatz von Bekanntem und Beherrschtem durch Unbekanntes,
- Austausch von Dienstleistern oder
- räumliche Verlagerung des Rechenzentrumstandortes der Systeme.

Bei Veränderungen werden von vielen Menschen zunächst die Risiken gesehen und die Chancen ausgeblendet. Hierdurch können Widerstände gegen eine Migration entstehen, die eine Bedrohung für die erfolgreiche Durchführung der Migration darstellen. Durch eine rechtzeitige und aktive Informationspolitik, in der den Mitarbeitern die Veränderung und die Gründe und Motivation hierfür aufgezeigt werden, können unbegründete Ängste und Gerüchte vermieden werden.

Der Informationsaustausch sollte im Dialog erfolgen, so dass die Ängste, Bedenken und Vorschläge der Mitarbeiter aufgenommen und im weiteren Migrationsvorgehen berücksichtigt werden können. Insbesondere bei ablösenden Migrationen und Konsolidierungen kann es nach Abschluss der Migration auch Mitarbeiter geben, für die die Veränderungen negative Auswirkungen haben. Dieses sollte zunächst identifiziert werden.

Je nach Art um Umfang der Veränderung sind flankierende Maßnahmen notwendig, die die Mitarbeiter auf die Veränderung vorbereiten beziehungsweise geeignet sind, eine Schlechterstellung einzelner Mitarbeiter zu kompensieren. Gutes Veränderungsmanagement innerhalb der IT kann die Akzeptanz der Migration nachhaltig absichern und so ein wesentliches Element zum Migrationserfolg sein.

### 3.8.6 Veränderungsmanagement innerhalb der Anwenderorganisation

Die Anwender sind bei Migrationen innerhalb der Planungs- und Umsetzungsphase nur partiell in die Aktivitäten eingebunden. Bei technischen Migrationen, die zu keinen Veränderungen bei den Prozessen, den Arbeitsweisen oder dem benötigen Know-How der Anwender führen, wird kein Veränderungsmanagement für die Anwender benötigt.

Hat die Migration hingegen Auswirkungen auf die Anwender, wirken üblicherweise einzelne Anwendervertreter an der Migration mit, um die Bedürfnisse der Anwender zu vertreten und sicherzustellen, dass das Migrationsergebnis praktisch nutzbar ist und den tatsächlichen Anforderungen entspricht.

Für die Anwender, die nicht aktiv an der Migration mitwirken, wird die Migration häufig erst mit der Umstellung sichtbar. Um abzuschätzen, ob die Anwender aktiv auf die Migration vorbereitet werden müssen, ist zu prüfen, ob sich wesentliche Veränderungen in den Bereichen

- Arbeitsabläufe oder Prozesse,
- Ansprechpartner oder Organisationseinheiten oder
- Bedienung der Anwendung

ergeben.

Durch ein entsprechendes Einführungs- und Schulungskonzept können, wie in 3.8.7 dargestellt, die fachlichen und organisatorischen Voraussetzungen geschaffen werden, um eine Migration erfolgreich durchzuführen und die neue Anwendung anschließend produktiv und reibungslos zu nutzen.

Resultieren aus der Migration Veränderungen für die Anwender bei den Arbeitsabläufen oder Verantwortlichkeiten, fallen Aufgaben für Anwendergruppen weg oder werden neue geschaffen, dann müssen die Anwender auf diese Veränderungen vorbereitet werden. Die Akzeptanz der Veränderung durch die Anwender ist wesentliche Voraussetzung für den Erfolg.

Eine frühzeitige Einbindung der Anwender über eine aktive Informationspolitik, in der die Gründe für die Veränderungen und das geplante Vorgehen dargestellt werden, ist ein wesentliches Element des Veränderungsmanagements. Insbesondere bei organisatorischen Veränderungen ist die Management-Unterstützung für das Migrationsprojekt eine wichtige Voraussetzung, da die Gefahr besteht, dass einzelne Einheiten Referats-, Abteilungs- oder Bereichsegoismus den Veränderungen entgegenarbeiten. Die Bedeutung der Unterstützung durch das Management wird in 3.8.9 detailliert dargestellt.

### 3.8.7 Einführungs- und Schulungskonzept

Durch eine Migration können sich Veränderungen sowohl für die Anwender als auch für die Betreiber der Anwendung ergeben. Werden durch eine Migration neue oder stark veränderte Verfahren eingeführt, dann muss im Rahmen einer erfolgreichen Migration sichergestellt sein, dass die Anwender darauf vorbereitet und entsprechend geschult sind. Kriterien bei der Erarbeitung eines angemessenen Einführungs- und Schulungskonzept für die Anwender ergeben sich aus den folgenden Punkten:

- Erfahrung und Reife der Anwender im Umgang mit IT-Systemen,
- Anzahl und räumliche Verteilung der betroffenen Anwender,
- Einfluss auf und Bedeutung der Änderungen für die Arbeitsabläufe der Anwender,
- Zeitpunkt der Migration und
- Belastung der Anwender während der Migrationszeit.

Aus diesen Kriterien kann die Form des Schulungs- und Einführungskonzeptes abgeleitet werden. Bei der Schulungsform kann zwischen Präsenzschulungen oder der Bereitstellung von Schulungsmaterial zum Selbstlernen entschieden werden. Es ist zu prüfen, ob eine Schulungsumgebung benötigt wird, in der die Anwender vor Abschluss der Migration bereits Erfahrungen mit der neuen Anwendung sammeln können. Beim Kreis der zu schulenden Personen gilt es zu entscheiden, ob alle Personen geschult werden ober ob mit Multiplikatoren gearbeitet wird.

Als Multiplikatoren wird ein ausgewählter Kreis von Anwendern bezeichnet, die intensiver geschult werden. Sie haben bei der Einführung der Anwendung die Aufgabe, die Schulung der Kollegen vor Ort zu übernehmen und als erste Ansprechpartner zu dienen. Die Belastung für die Multiplikatoren ist dabei zwar höher, aber durch die tiefergehenden Schulungen wird bei diesen Personen Expertenwissen aufgebaut, welches die zukünftige Nutzung der Anwendung unterstützt. Schulungs- und eventuell Reiseaufwendungen für alle Anwender können verringert werden, indem die Einweisung durch die Multiplikatoren am Arbeitsplatz im Rahmen der normalen Bürotätigkeit erfolgt.

Üblicherweise werden die genannten Optionen in Mischformen zu einem zur Migration passenden Schulungs- und Einführungskonzept für Anwender zusammengestellt.

Werden durch die Migration neue Technologien, Supportprozesse oder Aufgaben im Anwendungssupport eingeführt, dann muss sichergestellt sein, dass der IT-Betrieb und der Anwendungssupport hierauf vorbereitet sind. Analog zum Schulungskonzept sind für die betroffenen Personenkreise Einführungs- und Schulungsmaßnahmen zu planen.

Während der Einführungsphase ist mit einem erhöhten Unterstützungsbedarf für die Anwender sowie mit dem Auftreten von unvorhergesehenen Fehlern zu rechnen. Diesem sollte über eine entsprechende Planung von zusätzlichen Personalressourcen und gegebenenfalls externer Unterstützung Rechnung getragen werden.

### 3.8.8 Stakeholder

Im Vorfeld einer Migration muss analysiert werden, wer von der Migration betroffen ist. Die so analysierten Anspruchsgruppen (engl. Stakeholder) sind über eine gezielte Informationspolitik frühzeitig in die Migration einzubeziehen und wenn sinnvoll in das Projekt einzubinden.

Die wichtigsten Stakeholder für IT-Migrationsprojekte im öffentlichen Bereich sind

- die Behördenleitung,
- Entscheidungsträger aus den Fachbereichen und der IT,
- Anwender,
- IT-Mitarbeiter,
- der Personalrat,

- der Beauftragte für den Datenschutz,
- der Beauftragte für IT-Sicherheit,
- Politiker,
- Bürger und Unternehmen und
- die Öffentlichkeit.

Eine Akzeptanz des Migrationsprojektes bei den jeweiligen Stakeholdern ist ein kritischer Erfolgsfaktor. Die im Risikomanagement identifizierten Risiken sind eine Eingangsgröße für die Einbindung der Stakeholder. Nach der Identifikation der Stakeholder sollte im Risikomanagement überprüft werden, ob alle relevanten Risiken aus der Perspektive der Stakeholder identifiziert sind.

Die Einbindung der Stakeholder in das Migrationsprojekt bindet sowohl Projektressourcen als auch Ressourcen auf Seiten der Eingebundenen. Hier muss individuell entschieden werden, mit welchen Maßnahmen informiert und auch eingebunden werden kann, ohne dabei die Stakeholder zu überfordern. Geeignete Maßnahmen sind Informationsveranstaltungen, Newsletter und Informationsportale.

### 3.8.9 Management-Unterstützung

Im Idealfall führt eine Migration zu Verbesserungen, ohne dass sich Verschlechterungen ergeben, so dass alle Beteiligten reibungslos an der Migration mitwirken. Allerdings erzeugen Migrationen im Vergleich zum Tagesgeschäft selbst in diesen Fällen zusätzlichen Aufwand, so dass die Migration mit dem Tagesgeschäft und anderen Projekten um Ressourcen konkurriert. Dies gilt erst recht bei Migrationsvorhaben mit zumindest zeitweiser Verschlechterung der Arbeitsbedingungen von Anwendern, IT-Mitarbeitern oder sonstigen wesentlichen Stakeholdern.

Je stärker die Veränderungen durch eine Migration sind und je größer einzelne Einheiten oder Personen während oder nach der Migration Verschlechterungen im persönlichen Komfortbereich befürchten oder erfahren, desto wichtiger wird die Management-Unterstützung für die Migration. Die Migration bekommt nur dann die notwendigen Ressourcen, wenn sie eine entsprechende Priorität hat und der Projektleiter sich der Unterstützung seines Auftraggebers gewiss sein kann. Auftraggeber und Projektleiter sollten sich daher gegenseitig in kurzen Abständen über aktuelle Entwicklungen informieren und gemeinsam dafür Sorge tragen, dass das Vorhaben über entsprechenden Rückhalt innerhalb der Behördenleitung verfügt, um dem Projekt die notwendige Priorität zu verschaffen.

Die Notwendigkeit und der Umfang der Management-Unterstützung ist von der Größe und den Auswirkungen der Migration abhängig. Mögliche Maßnahmen zur Steigerung der Management-Unterstützung sind

- die regelmäßige Behandlung der Migration in Management-Runden,
- ein entsprechend besetzter Lenkungsausschuss und
- die Präsenz des Managements bei Kick-Off-Veranstaltungen, kritischen Meilensteinen und während der Einführung.

## 3.9 Sicherheitsaspekte

Behörden müssen die Sicherheit von Informationen von Gesetzes wegen gewährleisten[24]. Migrationsprojekte bieten das Potential, die IT-Landschaft hinsichtlich des Grads der Informationssicherheit nachhaltig zu verbessern. Es besteht aber das Risiko, dass durch mangelnde Planung das Sicherheitsniveau verringert wird, da sicherheitskritische Aspekte außer Acht gelassen werden. Zu Beginn muss sich die Frage gestellt werden, ob ein IT-Sicherheitskonzept vorliegt und welche Auswirkungen dieses auf die Migration hat.

### 3.9.1 Informationssicherheit

Informationssicherheit beinhaltet die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Aspekte wie Authentizität, Nachvollziehbarkeit und Verlässlichkeit können ebenfalls einfließen, sind aber nicht die Kernziele[25].

Der Datenschutz widmet sich dem Schutz personenbezogener Daten im Sinne des Bundesdatenschutzgesetz (BDSG), also u.a. einem Aspekt der Vertraulichkeit von Informationen als Teil der Informationssicherheit. Im Vordergrund des BDSG steht das grundsätzliche Verbot der automatisierten Verarbeitung personenbezogener Daten. Dies hat zur Konsequenz, dass personenbezogene Daten in den meisten Fällen nur mit der Einwilligung des Betroffenen oder auf gesetzlicher Grundlage erhoben, verarbeitet oder genutzt werden dürfen. Rechtmäßig erhobene Daten müssen ausreichend durch Maßnahmen gemäß den Schutzzielen der Informationssicherheit behandelt werden. Bei der Schutzbedarfsfeststellung (Unterabschnitt 3.9.3) ist insbesondere auch eine mögliche Verarbeitung von personenbezogenen Daten zu betrachten, um die datenschutzrechtlichen Rahmenbedingungen einzuhalten.

Zur unternehmensweiten Einhaltung von Informationssicherheit ist es notwendig, ein entsprechendes Managementsystem zu implementieren. Dafür bieten sich die Standards ISO 27001 „native“ oder ISO 27001 auf der Basis des vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten IT-Grundschutz-Katalogs an. Der IT-Grundschutz liefert sehr genaue Vorgaben, wie ein Managementsystem aufzubauen ist. In Organisationen wird ein Informationssicherheitsbeauftragter benannt, der für die Umsetzung der Vorgaben verantwortlich ist. Der Informationssicherheitsbeauftragte ist bei Migrationsprojekten gemeinsam mit dem Datenschutzbeauftragten frühzeitig einzubeziehen.

### 3.9.2 Schutzziele der Informationssicherheit

Informationssicherheit verfolgt das Ziel, Systeme und Daten hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit zu schützen. Die Begriffe bedeuten im Einzelnen:

**Vertraulichkeit** – Schutz vor unbefugter Kenntnisnahme

Informationen dürfen Personen, Entitäten oder Prozessen nicht unautorisiert zur Verfügung gestellt oder offenbart werden.

**Integrität** – Schutz vor Manipulation

Die Richtigkeit und Vollständigkeit von Informationen muss sichergestellt sein.

**Verfügbarkeit** – Schutz vor Informationsverlust

Informationen müssen einer berechtigten Einheit auf Verlangen zugänglich und für sie nutzbar sein.

Werden die Aspekte der Informationssicherheit frühzeitig in die Migrationsplanung aufgenommen, so sinkt das Risiko, die Schutzziele zu verfehlen. Hierfür ist das Migrationsprojekt in das bestehende Si-

[24] Siehe beispielsweise §§ 7, 9 Bundesdatenschutzgesetz
[25] Vgl. hierzu ISO 27001

cherheitskonzept einzubinden. Das BSI beschreibt in den IT-Grundschutz-Katalogen[26] die notwendige Strukturanalyse von IT-Organisationen, um Schutzklassen definieren zu können. Sofern kein Verfahren zur Einordnung eines Systems in die Sicherheitsstruktur vorhanden ist, muss letztere gebildet und das System anschließend darin eingeordnet werden, um den Anforderungen des IT-Grundschutzes zu genügen.

### 3.9.3 Strukturanalyse nach IT-Grundschutz

Die Strukturanalyse nach den IT-Grundschutz-Katalogen hat das Ziel, Systeme oder Systemverbünde gemäß ihrem Schutzbedarf zu kategorisieren. Dazu muss zunächst der Geltungsbereich definiert, also der zu betrachtende Verbund an Informationssystemen bestimmt werden. Sodann sind die einzelnen Objekte innerhalb des Informationsverbunds voneinander abzugrenzen und in Gruppen zu konsolidieren, deren Schutzbedarf gleich hoch ist. Für die Gruppen werden nun Regeln hinsichtlich der Schutzziele der Informationssicherheit hinterlegt. Diese Kategorisierung ermöglicht es, den Schutzbedarf einzelner Objekte über die Gruppierung sinnvoll darzustellen und das Sicherheitskonzept dahingehend auszurichten.

Um Anwendungen sicherheitstechnisch zu bewerten, wird jedem Schutzziel eine Schutzbedarfskategorie zugeordnet. In „BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise“ wird dazu die in Tabelle 3.1 dargestellte Einteilung vorgenommen.

Tabelle 3.1: Schutzbedarfsklassen

| **Kategorie** | **Bedeutung** |
|---|---|
| normal | Die Schadensauswirkungen sind begrenzt und überschaubar. |
| hoch | Die Schadensauswirkungen können beträchtlich sein. |
| sehr hoch | Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen. |

Der Schutzbedarf muss für jede IT-Anwendung anhand der von ihr verarbeiteten Daten ermittelt werden. Er orientiert sich an den gängigen Methoden des Risikomanagements und an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen IT-Anwendung bezüglich der unter Abschnitt 3.9.2 definierten Schutzziele verbunden sind.

### 3.9.4 Bewertungskriterien

Der Bedarf von Maßnahmen zur Erreichung von Informationssicherheit ergibt sich aus den Sicherheitsanforderungen an das System während der Migration und dem späteren Betrieb. Zu diesem Zweck befasst sich dieser Unterabschnitt mit Kriterien, die zur Planung und Zielerreichung der Informationssicherheit herangezogen werden können.

#### 3.9.4.1 Sicherheitskriterien zur Anforderungsanalyse

Vor der Initialisierung einer Migration ist zu prüfen, inwieweit die in Frage kommenden Migrationsalternativen die entsprechenden Sicherheitsanforderungen (z.B. in Bezug auf die Kommunikations-, Applikations- und Ausfallsicherheit) erfüllen. Für eine qualifizierte Aussage müssen Kriterien aufgestellt werden, die den tatsächlichen Bedarf widerspiegeln. Eine Auswahl möglicher Kriterien wird in der Tabelle 3.2 dargestellt, wobei in jedem Fall Verfügbarkeit, Vertraulichkeit und Integrität als Grundgerüst der Informationssicherheit geprüft werden müssen. Alle weiteren Kriterien sind als optional zu betrachten

[26] https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html

und je nach Migrationsobjekt anwendbar. Da Kriterien je nach Anwendungsobjekt eine unterschiedliche Relevanz haben, kann eine Gewichtung vorgenommen werden.

Tabelle 3.2: Sicherheitskriterien zur Anforderungsanalyse

| **Kriterium** | **Relevanz** | | |
|---|---|---|---|
| | niedrig | mittel | hoch |
| **Verfügbarkeit:** Eine Information muss zu demjenigen Zeitpunkt an demjenigen Ort verfügbar sein, an welchem sie benötigt wird. | | | |
| **Vertraulichkeit:** Eine Information darf nur denjenigen Personen zur Verfügung stehen, welche darüber aufgrund ihrer Aufgabenstellung verfügen sollen. | | | |
| **Interne Integrität (Konsistenz):** Eine Information darf durch Abbildungs- und Verarbeitungsvorgänge nicht verändert werden. Durch diese Vorgänge dürfen auch keine Widersprüche und Unvollständigkeiten entstehen. | | | |
| **Externe Integrität (Kongruenz):** Informationen müssen den Teil der Realität, welchen sie abbilden sollen, auch derart abbilden, dass keine Widersprüche zwischen der erkennbaren Realität und ihrer Abbildung entstehen. | | | |
| **Effizienz:** Eine Information soll so aufgebaut sein, dass sie sich mit minimalem Ressourceneinsatz nutzen lässt. | | | |
| **Verbindlichkeit:** Eine Information muss von Sender und Empfänger gleichermaßen anerkannt werden. | | | |
| **Datensicherheit:** Eine Information darf nur für diejenigen Zwecke verwendet werden, welche bei ihrer Erhebung angegeben oder beabsichtigt wurden. (Zweckbindung nach BDSG) | | | |
| **Anonymität:** Informationen müssen anonymisiert erhoben und verarbeitet werden, sofern §3 (6) oder (6a) BDSG Anwendung findet. | | | |
| **Authentizität:** Die Echtheit der Informationen muss gewährleistet sein. | | | |
| **Schutz vor Sabotage:** Informationen müssen physisch und logisch vor Sabotage geschützt werden. | | | |
| **Fälschungssicherheit:** Informationen müssen sicher vor Fälschung sein. | | | |
| **Funktionssicherheit:** Informationen dürfen nicht durch technische Fehler oder Fehlbedienung verloren gehen. | | | |

#### 3.9.4.2 Sicherheitskriterien zum Migrationsprojekt

Neben den Kriterien zur Bewertung der Anforderungen ist es notwendig, das Projekt und dessen Dokumentation hinsichtlich der Informationssicherheit zu prüfen. In der Regel geschieht dies durch den Informationssicherheitsbeauftragten der Organisation, der die Fragen zum Sicherheitsmanagement und Sicherheitskonzept beantworten kann.

Der Informationssicherheitsbeauftragte hat die Aufgabe, das Migrationskonzept hinsichtlich der Schutzziele und der getroffenen Maßnahmen zum Schutz von Informationen zu prüfen und ggf. Anpassungen vorzunehmen. Je nach Schutzbedarfsklasse ist zu prüfen, inwieweit die Sicherheitsanforderungen des BSI (beispielsweise hinsichtlich Einsichtnahme in Quellcodes, Sicherung der Kommunikationskanäle, etc.) erfüllt sind. Hierfür müssen folgende Fragestellungen Anwendung finden:

- Wie wird die Datenübertragung gesichert? Werden sichere Protokolle eingesetzt?
  Kommunikationswege müssen gegen unbefugten Zugriff gesichert sein. Der Zugriff auf Daten muss kontrolliert erfolgen. Der IT-Grundschutz bietet einen eigenen Maßnahmenkatalog mit konkreten Handlungsanweisungen für anwendbare Maßnahmen im Bereich der Kommunikation[27].
- Wie anfällig ist die Software für externe Angriffe, Viren und ähnliches?
  Je mehr Marktanteil eine Software hat, desto höher ist die Gefahr, dass Schadsoftware dafür entwickelt und eingesetzt wird. Die Prüfung der Common Vulnerabilities and Exposures (CVE) anhand öffentlich zugänglicher Datenbanken ist eine notwendige Maßnahme zur Bestimmung der Schwachstellen einer Software[28].
- Ist die Software modular aufgebaut?
  Ein modularer Aufbau von Software bietet Vorteile durch erhöhte Flexibilität, wenn System- oder Anwendungsprogramme verändert werden. Auch können durch mehrere Module die jeweils benötigten Zugriffe gezielt gesteuert werden.
- Wie anfällig ist sie für externe Angriffe, Viren und so weiter?

#### 3.9.4.3 Umsetzungsbewertung der Anforderungskriterien

Der Umsetzungsgrad der Sicherheitskriterien aus der Anforderungsanalyse ist während und nach erfolgter Migration zu prüfen, um Nacharbeiten oder mögliche Schwachstellen frühzeitig zu erkennen und durch geeignete Maßnahmen abzustellen. Sollten Maßnahmen nicht den gewünschten Effekt haben, müssen die verantwortlichen Personen eine Bewertung von Alternativen vornehmen.

Ziel der Bewertung ist es, Folgeaktivitäten gemäß Einfluss auf die Informationssicherheit zu priorisieren. Das migrierte System muss technisch und organisatorisch die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit erfüllen, um die Aufrechterhaltung des Sicherheitsmanagements zu gewährleisten. Die aus Unterabschnitt 3.9.4.1 „Sicherheitskriterien zur Anforderungsanalyse“ gewählten Kriterien müssen hinsichtlich des Erfüllungsgrads durch den Sicherheitsbeauftragten und die Fachbereiche bewertet werden. Hierfür kann das Bewertungsschema aus Tabelle 3.3 genutzt werden.

Tabelle 3.3: Bewertungsskala Erfüllung von Sicherheitskriterien

| Bewertung | Bedeutung | Handlungsbedarf |
|---|---|---|
| 0 | Keine Mängel | Kein Handlungsbedarf |
| 2 | Leichte Mängel | Risiken müssen bewertet werden. |
| 4 | Mittlere Mängel | Es besteht Änderungsbedarf, der mittelfristig umzusetzen ist. Die Dokumentation möglicher Maßnahmen kann nachgelagert zum Projekt erfolgen. |
| 6 | Schwere Mängel | Anpassungen sind dringend notwendig, um die Anforderungen der Informationssicherheit einzuhalten und das Migrationsprojekt abzuschließen. Die Maßnahmen sind entsprechend zu dokumentieren. |

Wenn die Schutzziele aus Unterabschnitt 3.9.2 und die daraus resultierenden Anforderungen an das System durch geeignete Sicherheitsmaßnahmen erfüllt sind, kann das Migrationsprojekt aus Sicht des Informationssicherheitsmanagements abgeschlossen werden. Offene Punkte müssen erfasst und nachfolgende Schritten bearbeitet werden.

[27] IT-Grundschutz M 5: Maßnahmenkatalog Kommunikation
[28] Siehe auch 4.3.2.3

## 3.10 Exkurs: Erfahrungsbericht der Landeshaupstadt München – Projekt LiMux

### 3.10.1 Historie und Ziele des Projekts LiMux

Die Landeshauptstadt München vollzieht bis 2013 einen umfassenden IT-Migrationsprozess[29]. Es gilt, alle rund 16.000 PC-Arbeitsplätze auf eine Open Source basierte, standardisierte und konsolidierte Lösung umzustellen. Der im Jahr 2003 durch den Münchner Stadtrat eingeschlagene Weg stützt sich auf drei grundsätzliche Entscheidungen:

1. ein freies und quelloffenes Betriebssystem inkl. einer Bürokommunikation, basierend auf offenen Standards für alle Arbeitsplatz-PCs,
2. die Maßgabe, künftig alle Fachverfahren plattformoffen zu beschaffen oder zu entwickeln,
3. eine standardisierte IT Plattform mit konsolidierten Anwendungen und Datenbeständen.

Im Frühsommer 2004 wurde der Startschuss für die konkrete Migration mit folgenden Zielen gegeben:

1. Durchführung der Migration der weit überwiegenden Anzahl der PC-Arbeitsplätze auf den stadtweit einheitlichen LiMux Client Bevorzugt werden dabei herstellerunabhängige und von einem bestimmten Betriebssystem und Office-Produkt unabhängige Lösungen
2. Migration der Fachverfahren auf webbasierte Lösungen bzw. auf native Linux-Lösungen, um für zukünftige Migrationen gerüstet zu sein
3. Konsolidierung und ggf. Migration der PC-Standard-Anwendungen auf ein vernünftiges Maß, d.h. eine Software für eine Funktion
4. Konsolidierung und Migration von MS-Office Makros, Vorlagen und Formularen, die im Lauf der Jahre in einer Vielzahl unkoordiniert und unkontrolliert entstanden waren
5. Einführung von Systemmanagement-Lösungen für den Basisclient, wie z.B. einer stadtweiten Softwareverteilung und eines einheitlichen Anmeldedienstes

Als Ergebnis der Migration sollen die aus der Historie bestehenden Abhängigkeiten von proprietären Produkten zunehmend aufgelöst werden und die Software- und Architekturauswahl langfristig die gewünschte Flexibilität gewinnen. Die Verwendung aufeinander abgestimmter Produkte eines Herstellers bietet in der Regel zwar den Komfort, dass Funktionen gemeinsam genutzt werden oder (proprietäre) Dateiformate durchgängig verwendet werden können. Andererseits wird damit die Ablösung dieser Produkte deutlich erschwert und weitere Produkte des selben Herstellers präjudiziert. Dadurch werden vermeidbare Kosten und Abhängigkeiten erzeugt. Letztlich führt dies zu einer deutlich eingeschränkten Freiheit bei der Auswahl geeigneter IT-Systeme in der eigenen Organisation. Das Projekt LiMux gilt zudem als „Blaupause“ für die Projektkultur zukünftiger IT Projekte.

### 3.10.2 Projektinhalt/Projektgegenstand

In einer Vorstudie wurden in den Jahren 2002 und 2003 besonders die technische und organisatorische Ausgangssituation geklärt.

[29] Siehe http://www.muenchen.de/Rathaus/dir/limux/index.html

#### 3.10.2.1 Heterogenität der Clients

Die Münchner Stadtverwaltung zeichnete sich vor der LiMux-Migration durch eine sehr heterogene IT-Technik aus. Die mittlerweile ca. 16.000 Benutzerrinnen und Benutzer arbeiteten seit Jahren mit dem Betriebssystem Windows-NT der Firma Microsoft und dem passenden Office-Produkt in unterschiedlichen Versionen von 97 bis 2000. Für die Erfüllung der vielfältigen Spezialaufgaben einer öffentlichen Verwaltung sorgten ca. 340 Fachverfahren, davon waren ca. 170 großrechnerbasiert. Zusätzlich wurden 300 Standardsoftwareprodukte eingesetzt.

#### 3.10.2.2 Zwei verschiedene Fileservice-Systeme

Der Fileservice basierte vor den Migrationsarbeiten auf zwei unterschiedlichen Konzepten, die von je circader Hälfte der städtischen Referate eingesetzt wurden. Einerseits wurde Netware von Novell in unterschiedlichen Versionen verwendet, andererseits wurden NT-Domänen-Emulationen wie zum Beispiel „PC-Netlink“ oder „Advanced Server for Unix“ eingesetzt.

#### 3.10.2.3 Zentrale Strategie und dezentraler Berieb

Organisatorisch ist in Münchens IT zwischen zwei Zuständigkeitsbereichen zu unterscheiden. Die IT-Strategie und die Beschaffung werden zentral koordiniert und entschieden, während der Betrieb und die Planung in 22 eigenständigen IT-Abteilungen der Stadt bewerkstelligt werden. Daraus ist leicht ersichtlich, dass es unterschiedliche Betriebs-, Benutzerverwaltungs- und Supportkonzepte gibt. Parallel zum LiMux-Projekt wurde vom Münchner Stadtrat das Projekt MIT-KonkreT zur strategischen Neuausrichtung der gesamten städtischen IT aufgesetzt.

#### 3.10.2.4 Bestandteile des linuxbasierten PC Arbeitsplatzes

Der LiMux Client ist ein Betriebssystem, das gezielt an die Bedürfnisse der städtischen Benutzerinnen und Benutzer angepasst ist. Das Betriebssysstem basiert aktuell auf einer Ubuntu 10.4 Distribution und der graphischen Oberfläche KDE 3.5 (Stand Herbst 2011). Dies bedeutet für die Mitarbeiterinnen und Mitarbeiter konkret, dass im Startmenü die einschlägigen Fachverfahren direkt ansteuerbar sind, dass bekannte und zusätzliche Anwendungsprogramme wie OpenProj, Freemind, Gimp, Acrobat Reader u.a. zur Verfügung stehen und dass unter LiMux der Desktop weitgehend die gleichen Funktionen wie der gewohnte Microsoft Windows-Desktop hat. Als Browser kommt Firefox und als E-Mail Client Thunderbird zum Einsatz.

Eine stadtweite Kollaboration Lösung wird derzeit in einem weiteren Projekt in Abstimmung mit LiMux realisiert. Die freie Bürosoftware OpenOffice.org (Version 3.2.1; Stand Herbst 2011) ersetzt die vergleichbaren Programme von Microsoft. Das Arbeiten mit Texten (writer statt word), Tabellen (calc statt excel), Präsentationen (impress statt power point) und zusätzlich Zeichnungen (Draw) ist wie gewohnt möglich. Im Sinne des Community Gedankens von „Geben und Nehmen“ hat die Landeshauptstadt ein Dokumenten- und Vorlagensystem WollMux entwickelt, unter der European Public Licence (EuPL) lizensiert und der Öffentlichkeit zur freien Nutzung zur Verfügung gestellt[30].

### 3.10.3 Projektsteuerung

Das Projekt LiMux wird mit einem klaren Governance Modell betrieben. Dieses rollenbasierte Leitungsmodell und seine Verantwortlichkeiten wurde schrittweise errichtet und weiterentwickelt.

Als oberstes Entscheidungsgremium fungiert der Lenkungskreis (LKr) mit seinem die Projektleitung beratenen Organ, dem sog. 3+1+2-Beirat. Der Lenkungskreis als oberstes Entscheidungsorgan setzt sich aus Bereichsleitern der Migrationsbereichen zusammen und wird von der 2. Bürgermeisterin geleitet. In der erweiterten Projektgruppe (ePG) sind alle Projektleiter aus den Migrationsbereichen vertreten. Hier wird über Form und Zeitpunkt der Migration sowie über technische Lösungen beraten. Die Projektgrup-

[30] http://www.WollMux.org

pe des Kernteams LiMux ist das zentrale Steuerungs- und Koordinationsorgan. Auf der Arbeitsebene sind zahlreiche Arbeitsgemeinschaften im Einsatz (AG LiMux Client, AG Office, AG Testmanagement, Kommunikationsmanager Netzwerk). Mitglied in den AGs sind die zuständigen Technikmanager aus den 22 Migrationsbereichen. Ein Change Advisory Board (CAB) regelt die Abstimmung im Change-Releasemanagement zwischen den betroffenen Bereichen.

Diese rollenbasierten Einheiten werden über eine klare Regelkommunikation gesteuert: Im zweimonatig tagenden Lenkungskreis wird über den Projektfortschritt berichtet, Jahres- und Zwischenziele vereinbart und gravierende Probleme einer Lösung zugeführt. In den Sitzungen der erweiterten Projektgruppe werden alle technischen und organisatorischen Themen aus einer operativen Sicht entschieden. Alle anderen Meetings und AGs dienen dem Informationsaustausch und der konkreten Problemlösung.

### 3.10.4 Projektorganisation

Das LiMux Projektteam besteht aus einem Kernteam und einem erweiterten Projektteam. Das Kernteam umfasst insgesamt rund 25 Personen, die an der Entwicklung und Bereitstellung des LiMux Clients, dem Support für OpenOffice inkl. Umstellung von Formularen und Makros, sowie an der Weiterentwicklung und dem Support des WollMux arbeiten. Das Kernteam setzt sich organisatorisch aus den Fachgruppen Anforderungsmanagement, Entwicklung, Office-WollMux, erweitertes Office Supportzentrum, Migrationsunterstützung, Testmanagement, Releasemanagement / Architektur sowie Veränderung & Kommunikation zusammen. Eine Projektleitung und das Projektbüro steuern das Kernteam.

Das erweiterte Projektteam setzt sich aus vielen Kolleginnen und Kollegen aus den Migrationsbereichen zusammen, die dort die Anforderungen stellen, die Migration verantworten und die Anwender täglich unterstützen.

Über die gesamte Projektlaufzeit wurde und wird das Projekt LiMux von einer Reihe von externen Partnern unterstützt. Hierzu gehören Credativ GmbH, DBI Klarl & Schuler GmbH, Gonicus GmbH, IABG mbH, IBM Deutschland, Unilog (heute Logica Deutschland). Dadurch wurde und wird nicht nur eine gleichbleibende hohe Expertise gesichert, sondern auch der Wirtschaftsstandort München gestärkt.

### 3.10.5 Projektmethodik

In der Projektvorbereitungsphase fiel die Entscheidung für den Einsatz eines klassischen meilensteinbasierten Projektmanagements. Dieses wird bis heute praktiziert. Im Laufe des Projekts wurden allerdings Änderungen an Projektstruktur und -methodik vorgenommen. So wurden inhärente Projektaufgaben wie Anforderungs-, Release- und Testmanagement in eigenständige Rollen und Teams ausgelagert. Auch wurde der Fokus auf die Akzeptanz und Zufriedenheit der IT Betreuer und Endanwender durch ein eigenständiges Veränderungsmanagement gestärkt. Auch das Vorgehen in der Entwicklung wurde geändert. Heute kommt hier Agiles Programmieren (angelehnt an die SCRUM-Methodik) zum Einsatz.

Eine bewährte Konstante blieb eine flexible und in sich konsistente Regelkommunikation über alle Hierarchiebenen hinweg.

### 3.10.6 Projektvorgehen

In dem Projekt wurde und wird ein bedarfsorientierter und evolutionärer Ansatz anstelle eines sog. „Big Bang“ verfolgt. In diesem Sinne wurde der Wechsel des Betriebssystems und der Wechsel des Officeprodukts mittels des Konzepts einer Softmigration entkoppelt. Zudem wurde in allen Migrationsbereichen zur Pilotierung der Migration eine so genannte „Keimzelle“ mit ca. 50 Rechnern installiert. Eine serielle Migration schließlich ermöglichte es den Projektteams, eine an den Bedürfnissen der Referate ausgerichtete Umstellung zu ermöglichen.

Vor allem in den großen und komplexeren Bereichen der Stadtverwaltung bot es sich an, im Rahmen einer „Softmigration“ nicht gleichzeitig auf den LiMux Client und OpenOffice.org umzustellen, sondern zunächst das bisherige Officeprodukt der Firma Microsoft durch die freie Alternative OpenOffice.org zu

ersetzen. Die Benutzerinnen und Benutzer konnten sich so in aller Ruhe an ihr neues Handwerkszeug gewöhnen. Mit der weichen Migration wurde die Schulungssituation entzerrt. Zudem konnte in einigen Bereichen die Zeit genutzt werden, infrastrukturelle Voraussetzungen für den Wechsel auf den LiMux Client zu schaffen.

Zunächst migrierten kleine und nach technischen Gesichtspunkten bei der Umstellung unkritische Bereiche innerhalb eines Migrationsbereiches, sog. „Keimzellen“. So konnten die Referate erste Erfahrungen mit der neuen Welt machen und den Entwicklern und dem erweiterten Office Supportzentrum mögliche Stolpersteine aufzeigen. Parallel zur Installation der Keimzellen lief die Umstellung der Bürokomunikation von MS Office auf OpenOffice.org auf allen PC Arbeitsplätzen. In den Jahren 2007-2009 sind alle PC Arbeitsplätze mit OpenOffice.org ausgestattet worden. Mit den Releases 2.3 und 2.4 des LiMux Client erfolgte dann eine verstärkte Phase der Migration in vielen Migrationsbereichen auf das linuxbasierte Betriebssystem. Mittlerweile ist das Release 4.0 mit aktuellem Thunderbird sowie Firefox Browser und OpenOffice 3.2.1 als Bürokommunikation auf über 8.000 PC Arbeitsplätzen im Einsatz (Stand Herbst 2011).

Die Landeshauptstadt München hat durch die Migration der Bürosoftware die Chance genutzt, die vorhandenen Vorlagen, Formulare und Makros zu konsolidieren, Redundanzen zu erkennen und den WollMux als stadtweites Vorlagensystem einzuführen.

# Kapitel 4

# Migrationsgebiete

Der Migrationsleitfaden beleuchtet verschiedene Software-Gattungen, die bei Migrationsvorhaben von Bundesbehörden regelmäßig berührt werden. Insbesondere soll er dort Hilfestellungen leisten, wo wesentliche Standards und zentrale Komponenten betroffen sind. Die Detailtiefe der Beschreibung der jeweiligen Software-Gattung richtet sich nach deren Relevanz für das Gesamtsystem und nach dem Grad der Standardisierung.

## 4.1 Übersicht

In Anlehnung an das technische Modell der Rahmenarchitektur IT-Steuerung Bund[1] werden die Themengebiete wie in Abbildung 4.1 dargestellt in verschiedene Bereiche unterteilt.

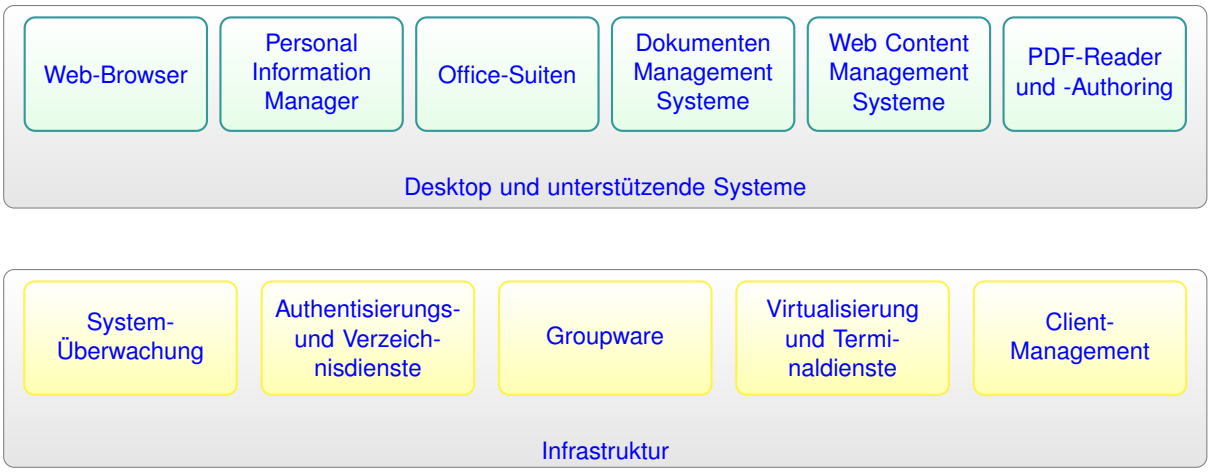


**Abbildung 4.1:** Migrationsthemen

Die Infrastruktur bildet den Grundstock eines IT-Systems, auf dem Dienste und Anwendungen aufbauen. Solche Dienste und Anwendungen mit allgemeinem, ressortübergreifenden Charakter werden im Abschnitt Desktop und unterstützende Systeme beschrieben. Auf die speziellen Migrationsaspekte von ressortspezifischen Diensten und Anwendungen (Fachanwendungen), die die grundsätzlichen strategischen, wirtschaftlichen und rechtlichen Betrachtungen im Migrationsleitfaden überschreiten, kann hier

[1] Siehe (Rat09)

nicht näher eingegangen werden[2]. Der Begriff *Dienst* ist in diesem Zusammenhang ein logisches Strukturelement im Sinne der o.g. Rahmenarchitektur und impliziert keine konkrete Technologie.

Für jedes Migrationsthema wird geprüft, welche Plattformen dafür genutzt werden können. Dabei wird für die Bereitstellung von Diensten auf die Plattformen Microsoft Windows und Linux eingeschränkt, für die Nutzung von Diensten wird das Apple-Betriebssystem MacOS X hinzugezogen.

### 4.1.1 Aufbau

Die Migrationsthemen sind ähnlich strukturiert, um das Lesen und Auffinden der gesuchten Informationen zu erleichtern, und gliedern sich in

1. Einleitung,
2. Kriterien,
3. Ist-Analyse,
4. Soll-Konzeption und
5. Produktauswahl.

Nach der Einleitung werden die Kriterien umrissen, die bei der Ist-Analyse und der Soll-Konzeption des Themas zu berücksichtigen sind, ggf. ergänzt um Hinweise auf domänenspezifische Aspekte. Nun werden die betrachteten Alternativen eines Migrationsthemas vorgestellt, die grundsätzlich nach Marktführerschaft, weitester Verbreitung im Behördenumfeld und verbreitetster Open-Source-Alternative ausgewählt werden, jeweils bezogen auf Deutschland. Da hier Überschneidungen möglich sind, können die Anzahl an betrachteten Alternativen variieren oder zweitplatzierte Alternativen hinzugezogen werden. Bei intensiv betrachteten Migrationsthemen werden zudem die alternativen Produkte anhand der aufgestellten Kriterien bewertet und daraus Empfehlungen abgeleitet.

Etwaige Empfehlungen beruhen ausschließlich auf der Bewertung der betrachteten Kriterien; kommen in einer Behörde weitere, insbesondere domänenspezifische Kriterien hinzu, können diese zu anderen Empfehlungen führen. Auch kann die stets notwendige Wirtschaftlichkeitsbetrachtung eine andere als die empfohlene Alternative als insgesamt günstigste Variante erscheinen lassen.

### 4.1.2 Bewertungs-Skalen

Die Bewertungskriterien werden unterschieden nach binären und abgestuften Ergebniswerten. Binäre Ergebniswerte sind Wertpaare wie „Ja / Nein“ oder „unterstützt / nicht unterstützt“ und werden dann zur Bewertung genutzt, wenn es auf das Vorhandensein einer Eigenschaft ankommt. Die in den Bewertungstabellen dafür genutzte Skala ist in Tabelle 4.1 dargestellt:

Tabelle 4.1: Skala für binäre Bewertungen

| Zeichen | Bedeutung |
|---|---|
| ✓ | ja / vorhanden |
| - | nein / nicht vorhanden |

[2] Zur Plattformunabhängigkeit von Fachanwendungen siehe (Koo07).

Abgestufte Ergebniswerte erweitern eine solche Prüfung, indem sie die Eigenschaft in ihrer Ausprägung bewerten. Die Skalenbreite wird in Tabelle 4.2 dargestellt:

Tabelle 4.2: Skala für abstufende Bewertungen

| Zeichen | Bedeutung |
|---|---|
| ++ | sehr gut/wird vollständig unterstützt |
| + | gut/wird gut unterstützt |
| o | befriedigend/ wird im Wesentlichen unterstützt |
| - | schlecht/wird kaum unterstützt |
| -- | sehr schlecht/wird gar nicht unterstützt |

### 4.1.3 Bewertungsmethode

Die alternativen Produkte eines Migrationsthemas werden auf die Erfüllung der jeweils aufgestellten Kriterien hin geprüft. Da die Kriterien eines Migrationsthemas regelmäßig technischer Natur sind und beispielsweise die Einhaltung offener Standards oder die Verarbeitung bestimmter Dateiformate betreffen, wird meist die binäre Bewertungsskala verwendet. Für die Darstellung unterschiedlicher Qualitäten bei der Erfüllung eines Kriteriums kommt die abgestufte Skala zur Anwendung. Hierbei wird bei unterschiedlicher Bewertung im Text auf die konkrete Über- oder Untererfüllung hingewiesen.

Einem spezifischen Migrationsvorhaben steht es frei, über die hier enthaltenen Bewertungen hinaus weitere domänenspezifische Aspekte (s.u.)) hinzuzuziehen oder die Ergebnisse mit einer Nutzwertanalyse[3] anzureichern.

### 4.1.4 Domänen-Spezifika

Praktisch jedes Migrationsthema hat Aspekte, die für Migrationsentscheidungen einzelner Behörden oder Abteilungen relevant sind, jedoch keine Allgemeingültigkeit aufweisen oder sich zumindest in der Relevanz deutlich unterscheiden. Solche Domänen-Spezifika sind in den Bewertungen des Migrationsleitfadens daher nicht enthalten, sollten aber bei der Bewertung einer konkreten Migration berücksichtigt werden. Sind die Domänen-Spezifika bereits in der Wirtschaftlichkeitsbetrachtung enthalten, ist kein weiterer Handlungsbedarf geboten. Andernfalls sollte die im Migrationsleitfaden befindliche Bewertungstabelle um die spezifischen Kriterien erweitert, deren jeweilige Bewertung eingetragen und die Gewichtung über alle Kriterien/-gruppen hinweg angepasst werden.

[3] Siehe beispielsweise (Zan76)

## 4.2 Infrastruktur

Analog zur Basis-IT der Rahmenarchitektur IT-Steuerung Bund beschreibt die Infrastruktur grundlegende Lösungen, die von anderen Teilen des Gesamtsystems genutzt werden können. Solche Lösungen reichen vom Domain Name System (DNS) bis zur Virtualisierung und vom Netzwerkdruck bis zur Systemüberwachung.

Angesichts der schieren Vielfalt an Lösungen im Bereich der Infrastruktur beschränkt sich der Migrationsleitfaden auf die nähere Untersuchung der in Abbildung 4.2 dargestellten Themen und geht in der Einleitung auf einige sonstige Elemente gängiger Infrastrukturen ein.

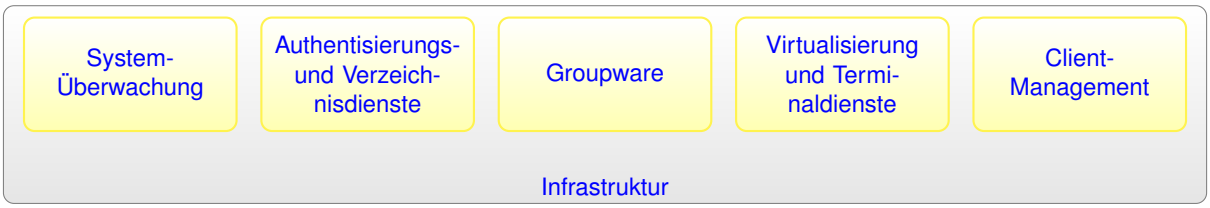


**Abbildung 4.2:** Migrationsthemen

In der letzten veröffentlichten Ausgabe des Migrationsleitfadens befasste sich das Modul II mit der IT-Infrastruktur. Die dort aufgeführten Themen „Authentisierungs- und Verzeichnisdienste“ und „System-Überwachungs- und -Management-Dienste“ werden in diesem Unterkapitel eingehend beschrieben, während die Themen „Datenbank-Systeme“ und „Webserver“ aufgrund der regelmäßig starken Verflechtung mit Fachanwendungen im Migrationsleitfaden nicht betrachtet werden (siehe entsprechende Ausführungen unter 4.1. Die sonstigen Themen „Netzwerkdienste“, „Dateiablage“ und „Druckdienste“ des o.g. Moduls II werden als Low-Level-Dienste nachfolgend kurz dargestellt.

### 4.2.1 Low-Level-Dienste

Als Low-Level-Dienste werden in diesem Migrationsleitfaden solche Dienste verstanden, die Ressourcen in ein Netzwerk einbinden, ohne sie – abgesehen von administrativen Funktionen – mit zusätzlicher Logik auszustatten. Low-Level-Dienste sind für das Funktionieren eines Netzwerks wesentlich und sollten daher in jedem IT-System vorhanden sein.

Das Internet und die meisten Behörden- und Firmen-eigenen Netzwerke nutzen heute das Internet Protocol (IP), häufig in Verbindung mit dem Transmission Control Protocol (TCP). Beide Protokolle sind offene Standards und werden bei der Internet Engineering Task Force (IETF) geführt. Für die darauf basierenden Low-Level-Dienste haben sich in den letzten Jahren offene Standards durchgesetzt, die ebenfalls von der IETF verwaltet und von allen betrachteten Betriebssysteme unterstützt werden. Eine nähere Untersuchung wesentlicher Kriterien und diese unterstützender Produkte ist für diese Dienste daher entbehrlich.

#### 4.2.1.1 Adress-Vergabe und Netzwerkkonfiguration

Alle Ressourcen eines Netzwerks benötigen eine eindeutige numerische Adresse, um gezielt angesprochen werden zu können. Abhängig von der IP-Version ist die Adress-Vergabe bereits im Protokoll geregelt (IPv6) und bedarf keiner weiteren administrativen Tätigkeiten, oder sie muss beim Einsatz von IPv4 gesondert über das Dynamic Host Control Protocol (DHCP) bereitgestellt werden. Letzteres dient bei beiden IP-Versionen überdies der Zuweisung der Netzwerkkonfiguration an sich daran anmeldende Ressourcen, beispielsweise die Zuordnung eines Rechnernamens oder die Bekanntgabe der Adressen von Diensten zur Namensauflösung (s.u.) oder zur Zeit-Synchronisation (ntp).

Sämtliche Linux-Distributionen und die Server-Betriebssysteme von Windows enthalten einen Standard-konformen DHCP-Server. Die Funktionalität eines DHCP-Clients ist bei Windows, Linux und Mac OS X ein Bestandteil des Betriebssystems. Aufgrund des offenen Standards sind die DHCP-Dienste und -Clients unter Windows, Mac OS und Linux vollständig kompatibel.

Bei der Umstellung des gegenwärtig noch eingesetzten IPv4 auf das künftige IPv6 gilt es zu beachten, dass die Verfolgbarkeit des einzelnen Anwenders durch die dauerhafte Vergabe eindeutiger IP-Adressen möglich wird. Dies ist aus Gründen das Datenschutzes nicht hinnehmbar. Bei der Konfiguration der Endgeräte muss daher darauf geachtet werden, dass die dafür vorgesehenen *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*[4] ggf. aktiviert werden. Dies ist für alle untersuchten Plattformen und auch für die meisten Mobil-Plattformen möglich[5].

#### 4.2.1.2 Namensauflösung

Damit Netzwerk-Ressourcen nicht über Zahlenreihen, sondern über einen Namen angesprochen werden können, muss der numerischen Adresse ein Name zugeordnet und die Zuordnung abgefragt werden können (Namensauflösung). Diese Aufgaben übernimmt das Domain Name System (DNS), ein weltweit verteilter hierarchischer Verzeichnisdienst, der den Namensraum des Internets und ggf. des eigenen Intranets verwaltet. Die Namensauflösung innerhalb eines Behördennetzes wird über im Intranet befindliche DNS-Server konfiguriert. Ggf. darüber hinaus gehende Anfragen reicht der interne DNS-Server an das weltweite DNS weiter.

Die Adressen der internen DNS-Server werden üblicherweise per DHCP verteilt und stehen damit allen Netzwerk-Ressourcen des Intranets für die Namensauflösung zur Verfügung (s.o.). Analog zu DHCP ist die Funktionalität für DNS-Abfragen ein Bestandteil aktueller Betriebssysteme. Sämtliche Linux-Distributionen sowie die Server-Betriebssysteme von Windows enthalten einen Standard-konformen DNS-Server, der zur Intranet-Namensauflösung genutzt werden kann.

#### 4.2.1.3 Dateiablage

Für die Ablage von Dateien im Intranet und für den gemeinsamen Zugriff darauf wird ein Fileserver benötigt, mit dem über bestimmte Protokolle kommuniziert wird. Der heute verbreitetste Standard für solche Zugriffe ist das von Microsoft entwickelte und inzwischen offengelegte Common Internet File System (CIFS), das frühere Server Message Block Protokoll (SMB). Microsoft bietet diese Möglichkeit als „Windows Server File Services“ an, unter Linux kann das OSS-Projekt SAMBA[6] für die Bereitstellung entsprechender Dienste genutzt werden. Client-seitig verfügen alle betrachteten Betriebssysteme über Funktionalitäten zum Zugriff auf Dateiablagen über CIFS/SMB.

Die reine Dateiablage bietet keine Funktionalität zur Versionierung einzelner Dateien oder zum Schutz vor gegenseitigem Überschreiben oder Löschen. Hierfür müssen ggf. weitere Dienste wie eine Versionsverwaltung oder sonstige Kollaborations-Lösungen eingesetzt werden.

#### 4.2.1.4 Druckdienste

Professionelle Drucker verfügen über eine Netzwerk-Schnittstelle, über die sie im Intranet genutzt werden können. Solche Drucker agieren selbst als Druck-Server und können regelmäßig über verschiedene Protokolle wie Internet Printing Protokoll (IPP), Common Unix Printing System (CUPS) und Line Printer Daemon Protocol (LPDP) angesprochen werden. Moderne Clients verfügen auf allen betrachteten Plattformen über die Funktionalität, um Netzwerk-Drucker über die o.g. Protokolle nutzen zu können.

Drucker ohne eingebauten Druck-Server können über einen angeschlossenen Rechner ebenfalls im Netzwerk bereitgestellt werden; allerdings muss hierzu ein Druck-Server auf diesem Rechner installiert und der Drucker für die Verwendung im Netzwerk freigegeben werden. Microsoft bietet diese Möglichkeit

[4] Siehe http://tools.ietf.org/html/rfc4941
[5] Siehe http://heise.de/-1204783
[6] http://www.samba.org

als „Windows Server Print Services“ als Teil des CIFS an, unter Linux kann wie für die Dateiablage SAMBA für die Bereitstellung entsprechender Dienste genutzt werden.

#### 4.2.1.5 Komplettlösungen und Distributionen

Komplettlösungen für die Infrastruktur werden in verschiedener Form angeboten. Allen gemeinsam ist, dass sie die oben genannten Low-Level-Dienste vollständig unterstützen. Sie unterscheiden sich allerdings in der Unterstützung der nachfolgend detaillierter beschriebenen Dienste (siehe dort) und auch bei den Lizenzmodellen.

##### 4.2.1.5.1 Microsoft Server 2008 R2

Microsoft Server 2008 R2 wird auf der Basis traditioneller Software-Lizenzen in verschiedenen Editionen mit unterschiedlichen Merkmalen und Preisen angeboten. Eine optimale Versorgung mit den tatsächlich für den jeweiligen Behördenbetrieb benötigten Lizenzen ist aufgrund deren Vielfalt und unterschiedlicher Abhängigkeiten nicht trivial[7] und sollte ggf. über entsprechend geschultes Personal oder externe Dienstleister bezogen werden. Der Quellcode der einzelnen Komponenten ist nicht offengelegt, es handelt sich durchweg um proprietäre Software (siehe 2.7). Microsoft unterstützt die einzelnen Versionen seiner Server-Distribution regelmäßig über mehrere Jahre hinweg. Gegen zusätzliche Kosten ist auch ein erweiterter Support über das allgemeine Unterstützungsende hinaus möglich.

##### 4.2.1.5.2 Linux-Distributionen

Alternativ dazu existieren verschiedene Anbieter sogenannter Enterprise Editionen auf der Basis von Linux, beispielsweise

- Debian GNU/Linux,
- Red Hat mit dem Red Hat Enterprise Linux (RHEL),
- Novell mit dem Suse Linux Enterprise Server (SLES),
- Canonical mit der Ubuntu Long Term Edition (Ubuntu LTE) und
- Univention mit dem Univention Corporate Server (UCS).

Diesen Linux-Distributionen ist gemeinsam, dass die jeweilige (Server-)Version über einige Jahre hinweg supported wird und die Software im Quellcode frei verfügbar, also Open-Source-Software ist. Einige der Distributionen können über ein Abonnement-Modell mit einfach gestalteten Lizenzen bezogen werden. Über solche Abonnements erhält der Käufer die Distribution in einer unmittelbar installierbaren Binärform, Zugriff auf technische Unterstützung und je nach Abonnement weitere Leistungen wie Rechtsschutz gegenüber Software-Patenten (*Legal Assurance*).

[7] Siehe http://www.microsoft.com/germany/windowsserver2008/r2-lizenzierung.mspx

Tabelle 4.3: Verbreitete Linux-Distributionen

| **Distribution** | **Debian** | **RHEL** | **SLES** | **Ubuntu LTE** | **UCS** |
|---|---|---|---|---|---|
| Sourcecode frei verfügbar | ✓ | ✓ | –[8] | ✓ | ✓ |
| Installationsfähiger Bezug | Frei | Abonnement | Abonnement | Frei | Abonnement |
| Lizenzierung | Keine | Je Server | Je Server | Keine[9] | Je Server & User |
| Support-Zeitraum (Jahre) | 1 ab Folge-Release[10] | 7 | 5 | 5[11] | 1, jährlich verlängerbar |
| Derivate, bspw. | Ubuntu, UCS, Knoppix | CentOS | – | Kubuntu, Edubuntu | – |
| Technologische Vorhut | Unstable, Testing | Fedora | openSUSE | Ubuntu Standard Edition | – |

[8] Der Sourcecode von openSUSE ist frei verfügbar.
[9] Über Ubuntu Advantage können den Abonnements von RHEL, SLES und UCS vergleichbare Zusatzleistungen bezogen werden.
[10] Siehe http://www.debian.org/security/faq#lifespan
[11] Siehe http://www.canonical.com/content/ubuntu-1204-feature-extended-support-period-desktop-users

## 4.2.2 System-Überwachung

### 4.2.2.1 Einleitung

Die heutigen Anwendungen und Verfahren sind darauf angewiesen, dass die IT-Infrastruktur und die IT-Anwendungen weitestgehend störungsfrei zur Verfügung stehen. Durch eine Überwachung der Serversysteme, Infrastrukturkomponenten und Anwendungen wird erreicht, dass drohende Störungen, die aufgrund von Frühwarnindikatoren vor ihrem Eintritt erkannt werden, durch Vorsorgemaßnahmen vermieden werden können. Treten dennoch Störungen ein, so werden diese durch die Überwachung zeitnah erkannt und können ohne Zeitverlust bearbeitet werden.

#### 4.2.2.1.1 Überwachungsklassen

In der Systemüberwachung werden unterschiedliche Überwachungsklassen implementiert, insbesondere die Überwachung

- der Verfügbarkeit von Servern, Leitungen oder anderen einzelnen Komponenten,
- der Auslastung,
- der Verfügbarkeit von Anwendungen oder Diensten,
- der Performance (Durchsatz oder Antwortzeiten) von Anwendungen,
- von Geschäftsprozessen und
- der Integrität der Infrastruktur.

In der heutigen Praxis sind nicht alle Überwachungsklassen durchgängig und vollumfänglich implementiert, die Überwachung der Verfügbarkeit ist jedoch als Mindeststandard gesetzt.

#### 4.2.2.1.2 ITIL-Bezug

Die Systemüberwachung ist ein Basisdienst, der sich aus der einfachen Netzwerküberwachung zu einer umfassenden Systemüberwachung weiterentwickelt hat. Dabei haben sich Standards wie das Simple Network Management Protocol (SNMP) zur Überwachung einzelner Komponenten etabliert, auf denen die Systemüberwachungswerkzeuge aufsetzen.

Die Systemüberwachung deckt die Aufgaben des ITIL-Prozesses *Event Monitoring* ab. Derzeit entwickeln sich verstärkt Lösungspakete, die neben der Systemüberwachung auch für Aufgaben anderer ITIL-Prozesse wie *Incident Management*, *Request Fulfillment*, *Configuration Management* und *Change Management* verwendet werden können.

#### 4.2.2.1.3 Schnittstellen zur Systemüberwachung

Für jede Systemüberwachungslösung sind die Schnittstellen zu den überwachenden Systemen die Grundvoraussetzung dafür, dass eine Überwachung eingerichtet werden kann. Eine stabile und gut dokumentierte Schnittstelle der zu überwachenden Systeme spielt eine zentrale Rolle.

Im Folgenden werden die wesentlichen Schnittstellen benannt, auf die sich sowohl die freien als auch die kommerziellen Systemüberwachungswerkzeuge stützen. Es gibt drei weit verbreitete universelle Schnittstellen:

- **SNMP** – Netzwerkkomponenten, Drucker und physische Sensoren sind über das *Simple Network Management Protokoll* ansprechbar.
- **WBEM** – Enterprise Unix/Linux Systeme und die Hardware, auf denen sie betrieben werden, sind über das freie Protokoll zum *Web Based Enterprise Management* ansprechbar.
- **WMI** – *Windows Management Instrumentation* ist die Microsoft'sche Implementierung von WBEM für Windows Server Systeme und Services und die darunterliegende Hardware.

Für einige anwendungsspezifische Bereiche existieren weitere relevante Schnittstellen:

- **JMX** – *Java Management Extensions* sind der Standard, über den Servlet Container und Java Application Server ihre Managementdaten bereitstellen. Die Schnittstelle kann von Anwendungen individuell erweitert werden.
- **Web Services** – Verschiedene Softwareprodukte wie VMware vSphere bieten eine Reihe von Web Services zu ihrer Verwaltung und Überwachung, die von Systemüberwachungswerkzeugen genutzt werden können.
- **CCMS**/**RFC** – Das *Computer Center Management System* dient zur Verwaltung und Überwachung von SAP-Systemen auf Windows, Unix und Linux.

Diese universellen und anwendungsspezifischen Schnittstellen sind die Bordmittel der jeweiligen Umgebung und werden von den Produktherstellern mehr oder weniger intensiv unterstützt. Gegenüber SNMP weisen WBEM und WMI einen deutlich größeren Umfang an Systeminformationen auf.

Während bei SNMP-basierten Überwachungsmodulen nur ein relativ einfacher Status signalisiert wird, steht unter WBEM eine detaillierte Auflistung der verschiedenen Systemkomponenten zur Verfügung, von einzelnen Lüftern über Betriebssystem-Dienste bis hin zur Auslastung einzelner Hardwarekomponenten. Auf verschiedenen logischen Ebenen befindliche Elemente lassen sich einzeln ansprechen und überwachen, beispielsweise die physische Festplatte, die Volume Group und das Logical Volume im Falle eines Raid Controllers. Zudem bringt die Hardware-Überwachung mit WBEM eine einheitliche Sicht auf die Hardware-Komponenten unterschiedlicher Hersteller über einen einheitlichen Zugriffsmechanismus. WBEM ist ein offener, von der Distributed Management Tast Force (DMTF) entwickelter Standard für das Systemmanagement. Mit WMI lassen sich außerdem applikationsspezifische Parameter abfragen. So bietet Citrix in seinen Produkten beispielsweise eine Schnittstelle, die Kenndaten wie die Anzahl der Nutzer für WMI aufbereitet.

#### 4.2.2.2 Kriterienkatalog

Über die generischen **Schnittstellen**-Standards und ihre applikationsspezifischen Pendants lassen sich über 90% des gesamten Überwachungsbedarfs abdecken. Bei der Einführung von neuen Anwendungssystemen sollte darauf geachtet werden, dass die Komponenten über die genannten Standardwege abgefragt werden können, da dann eine nahtlose Integration in eine bestehende Systemüberwachungslösung ohne großen Aufwand möglich ist.

Das Überwachungsspektrum sollte im laufenden Betrieb um neue Rechner, Netzwerk-Komponenten, Basis- und Querschnitts-IT auf der Basis o.g. Standard-Schnittstellen **erweitert** werden können. Neuartige Überwachungsschnittstellen und Berichtsarten sollten der Systemüberwachung **modular hinzugefügt** werden können. Dabei sollten diese Module mit weitgehend **beliebiger Technik** umgesetzt werden können, um die jeweilige Überwachungsanforderung mit vorhandenem IT-Personal und Wissen optimal umsetzen zu können.

Berichtsmöglichkeiten zur **Verfügbarkeit** und **Performanz** überwachter Elemente sollten dem Produkt beiliegen oder frei erhältlich sein. Die Überwachung einzelner Elemente sollte **einfach konfiguriert** werden können. Die Konfiguration sollte eine Unterscheidung nach **Wochen- und Feiertagen**, **Uhrzeiten**, **Eskalationszeiträumen** und **Alarmierungsarten** ermöglichen. Als Alarmierungsarten sollten mindestens **E-Mails** und **SMS** versandt werden können. Außerdem sollten **Verhaltensregeln** für unterschiedliche Intensitätsstufen der überwachten Werte angegeben werden können.

Verschiedene logisch zusammengehörige Elemente sollten für die Überwachung **gruppiert** und so **kaskadiert** werden können, dass Folgefehler als solche erkannt und redundante Meldungen vermieden werden. Die Systemüberwachung sollte sich gut in Lösungspakete zu weiteren ITIL-Themen wie dem o.g. Incident Management **integrieren** lassen.

#### 4.2.2.3 Methodik

Die Migration sollte mit der Analyse des **Ist-Zustands** beginnen und zunächst die Fähigkeiten und Unzulänglichkeiten der derzeit verwendeten Systemüberwachungslösung feststellen. Das derzeitige Überwachungsspektrum sollte nach der Art der überwachten Komponenten und der dazu verwendeten Schnittstellen klassifiziert werden. Die Anzahl der je Art überwachten Komponenten sollte ebenso festgestellt werden wie die Häufigkeit und Form der Zustandsfeststellung (z.B. aktiver HA-Heartbeat oder passiver Ping). Auch gilt es, die derzeit notwendigen Kenntnisse des IT-Personals bzgl. Anpassungen und Erweiterungen der vorhandenen Überwachungslösung ebenso zu ermitteln wie deren darüber hinausgehende Kenntnisse zu Skript- oder sonstigen Programmiersprachen.

Art und Umfang des aktuellen Berichtswesens der Systemüberwachung sollte fest- und dem tatsächlichen Bedarf gegenübergestellt werden. Außerdem sollten Informationen über geplante Systemerweiterungen und -änderungen eingeholt werden.

Der nächste Schritt ist die Konzeption des Soll-Zustands. Dieser sollte neben den bereits überwachten Elementen und deren Einzelwerten die noch nicht integrierten Komponenten samt deren Schnittstellen und Sensoren[12] umfassen. Daraus sollte hervorgehen, welche Sensoren über welche Schnittstellen künftig insgesamt integriert, welche Arten von Teilsystemen, Diensten und Anwendungen überwacht werden müssen und in welcher Häufigkeit zu welchen Tagen und Zeiten überwacht und mit welchen Maßnahmen in welchen Zeiträumen reagiert werden soll.

Es sollten alle künftig geforderten Berichtsarten samt deren Adressaten und ggf. notwendiger Aggregationen für verschiedene Berichtsebenen definiert werden. Die Aussagekraft einzelner Berichte sollte so präzisiert werden, dass Wertebereiche einzelner Sensoren klar umrissen sind, logische Kombinationen von Sensoren dargestellt und deren Zusammenwirken beschrieben werden. Neben Berichten über den aktuellen Systemzustand sollten die Anforderungen an statistische Auswertungen und darauf basierende Berichte festgelegt werden.

#### 4.2.2.4 Betrachtete Alternativen

Bei den zur Systemüberwachung eingesetzten Werkzeugen gibt es weite Leistungs- und Funktionsunterschiede. Die Produkte reichen von breit aufgestellten Werkzeugen, die einen großen Teil der Überwachungsklassen über einen heterogenen Bestand an Hardware- und Softwareinfrastruktur universell abdecken, bis hin zu spezialisierten Lösungen, die nur eine Überwachungsklasse für einen eingeschränkten Bereich von Infrastrukturkomponenten abdecken. Verlässliche Daten zur Verbreitung einzelner Lösungen gibt es nicht, die nachfolgende Auswahl basiert daher auf Schätzungen.

Näher betrachtet werden folgende Lösungen zur Systemüberwachung:

- CA NSM (ehemals Unicenter) als Marktführer,
- HP OpenView als in Behörden weit verbreiteter proprietärer Lösung und
- Nagios als am weitesten verbreiteter OSS-Alternative.

#### 4.2.2.5 Bewertung

Nachfolgend werden die o.g. Lösungen beschrieben und tabellarisch verglichen. Weitere Produkte zur Systemüberwachung werden außerhalb der Bewertung anschließend kurz vorgestellt.

##### 4.2.2.5.1 Nagios

Im Bereich der umfassenden Systemüberwachung, das heißt die Überwachung von Servern mit Blick auf Hardware und Software, Netzwerkkomponenten, WAN-Verbindungen und Applikationen hat sich mit

[12] Ein Sensor ist in diesem Zusammenhang eine beliebige Form der Ermittlung konkreter Werte von Hard- oder Softwarekomponenten.

Nagios[13] ein leistungsstarkes freies System etabliert, um das herum viele Erweiterungen und Ergänzungen entstanden sind. Eine ebenfalls freie Alternative mit einem annähernd vergleichbaren Leistungsumfang ist Zenoss[14]. Auf Basis von Nagios entstand Incinga[15] als eine alternative Weiterentwicklung, die eine nennenswerte Marktverbreitung erreicht hat.

Der Nagios-Kern bietet einen Weg, definierte Services überwachen zu lassen. In regelmäßigen Intervallen werden sogenannte Plug-Ins ausgeführt, die den Zielwert und den Istwert des überwachten Systems miteinander vergleichen. Nachgelagert kann durch die Ergebnisse der Prüfungen eine Alarmierung und Eskalation der Alarme durchgeführt werden. Nagios bietet dabei ein hohes Maß an Flexibilität und eine gute Erweiterbarkeit. Ein einfaches Plug-In kann bereits aus einem einfachen 10-zeiligen Shell-Skript bestehen.

Überwachungs-, Alarmierungs- und Eskalationszeiträume können individuell konfiguriert werden und z.B. für unterschiedliche Tageszeiten oder Wochentage und an Feiertagen ein anderes Verhalten aufweisen. Es können mehrere Alarmierungsgruppen eingerichtet werden, deren Verhalten in Abhängigkeit von Zeit und Überwachungsmeldung konfiguriert werden kann. Die eigentliche Alarmierung wird über weitere Plug-Ins durchgeführt. Der Standardweg der Alarmierung ist das Versenden von E-Mail; ein SMS-Versand oder Desktop-Notifications können mit wenig Aufwand eingerichtet werden.

Zur Strukturierung der Systemlandschaft bietet Nagios mehrere Möglichkeiten. In der Regel wird in Nagios ein Host hinterlegt, auf dem mehrere Services überwacht werden. Host-übergreifende Abhängigkeiten einzelner Services untereinander lassen sich genauso modellieren wie die Netzwerktopologie der einzelnen Hosts untereinander. Liegt eine Störung einer untergeordneten Komponente vor, so wird der durchzuführende Check einer übergeordneten Komponente automatisch vorgezogen, um Fehlalarmierungen zu vermeiden. Bei einer Störung im Netzwerkbereich ist so beispielsweise sichergestellt, dass eine Alarmierung zeitnah stattfindet, aber die Adressaten nicht mit redundanten Informationen überflutet werden.

#### 4.2.2.5.2 CA NSM

Computer Associates bietet im Rahmen seines Lösungsportfolios zur Unterstützung des IT Service Managements auch ein Werkzeug zur Überwachung und Bewertung heterogener Systemlandschaften. Das früher als CA Unicenter Network and Systems Management bekannte NSM[16] bietet die Möglichkeit, auf jede instrumentierte Datenquelle Alarme zu setzen und Reports zu erzeugen. Gut gelöst sind die Auswertungen der Performance Daten. Hier ist der Übergang zwischen kurzfristigen Zeiträumen und einer langfristigen Betrachtung fließend. Die zentralen Server der NSM-Umgebung sind in der Version 11 nicht nur unter Windows, sondern auch auf RedHat und SuSE Linux lauffähig. Im Portfolio sind unter anderem der Network and Systems Manager, Active Directory und zOS Monitoring sowie verschiedene Datenbanken. Die Lösung umfasst ein Portal, um auf alle Daten an zentraler Stelle zugreifen zu können. Weitere kostenpflichtige Optionen sind die Cluster- und VMware-Überwachung.

#### 4.2.2.5.3 HP OpenView

HP OpenView ist ebenfalls in ein breites Spektrum an ITSM Werkzeugen von einem Hersteller eingebettet. OpenView konzentriert sich auf eine Grundüberwachung, die mit applikationsspezifischen Plug-Ins ergänzt werden kann. Dabei hat OpenView durch eine bereits lange Präsenz am Markt den Vorteil, eine sehr umfangreiche Cross-Plattform Integration zu haben. Unter den Monitoring Plug-Ins findet sich auch das hauseigene OpenVMS, Documentum, Citrix und MySQL, um nur einige zu nennen. OpenView kann durch das von HP gelieferte SDK für eigene Anwendungen erweitert werden.

[13] http://www.nagios.org
[14] http://community.zenoss.org
[15] http://www.icinga.org
[16] http://www.ca.com/de/Client-Management.aspx

#### 4.2.2.5.4 Vergleich Systemüberwachungswerkzeuge

Tabelle 4.4: Vergleich Systemüberwachungswerkzeuge

| Werkzeug | **Nagios** | **CA NSM** | **HP OpenView** |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | ✓ | – | – |
| Lizenzkosten | – | verschiedene Lizenzmodelle | verschiedene Lizenzmodelle |
| Benötigte Plattformen[17]<br>Windows Server 2008 / Linux | –/✓ | ✓/✓ | ✓/✓ |
| **Konfiguration** | | | |
| Unterstützte Schnittstellen[18]<br>SNMP/WBEM/WMI/JMX/WebServices | ✓/✓/✓/✓/✓ | ✓/✓/✓/✓/✓ | ✓/✓/✓/✓/✓ |
| Vollständige Vertikale[19] | ✓ | ✓ | ✓ |
| Aufnahme neuer Elemente im laufenden Betrieb | ✓ | ✓ | ✓ |
| Konfigurations-Schnittstelle | Dateibasiert, Web-GUI[20] | Web-GUI | Web-GUI |
| Unterscheidung Wochen-/Feiertage | ✓ | ✓ | ✓ |
| Unterscheidung Uhrzeiten | ✓ | ✓ | ✓ |
| Vorgabe Eskalationszeiträume | ✓ | ✓ | ✓ |
| Gruppierung/Kaskadierung | ✓/✓ | ✓/✓ | ✓/✓ |
| Alarmierungsarten (E-Mail/SMS) | ✓/✓ | ✓/✓ | ✓/✓ |
| Konfigurierbare Verhaltensregeln | ✓ | ✓ | ✓ |
| **Erweiterbarkeit** | | | |
| Modularer Aufbau | ✓ | ✓[21] | ✓[21] |
| Wahlfreiheit Modul-Technik | ✓[22] | – | – |
| **Online-Überwachung** | | | |
| Verfügbarkeit | ✓ | ✓ | ✓ |
| Performanz | ✓[20] | ✓ | ✓ |
| **Berichtswesen** | | | |
| Aggregierte Berichte | ✓[20] | ✓[23] | ✓[23] |
| Statistiken | ✓[20] | ✓[23] | ✓[23] |

[17] Zur Installation der Überwachungssoftware
[18] Nativ oder über Erweiterungen
[19] Einbeziehung beliebiger Elemente vom Netzwerk-Knoten bis zur konkreten Anwendung.
[20] Über eine Erweiterung der Überwachungssoftware (Plug-In, AddOn o.ä.)
[21] Module unterliegen dem Releasemanagement des Herstellers und verursachen weitere Kosten.
[22] Plug-Ins können in beliebigen Skriptsprachen implementiert werden.
[23] Ggf. über Report Generator

#### 4.2.2.5.5 Sonstige Werkzeuge

IBM Tivoli ist eingebettet in eine Reihe von IBM Client-Management Werkzeugen. Vor allem zu nennen ist das unter dem Namen Tivoli Storage Manager firmierende Backup Werkzeug. Tivoli bietet ähnlich weitreichende vorgefertigte Plug-Ins wie OpenView. Zusätzlich liefert IBM ein GUI basiertes Werkzeug, das verspricht, eigene Software Services einfach in Tivoli aufzunehmen. Tivoli Monitoring glänzt mit der Möglichkeit, Performance Verläufe vorrausschauend zu betrachten und gegebenenfalls bereits im Vorlauf einer Grenzüberschreitung einen Alarm auszulösen.

Microsoft Operations Manager (MOM) ist eine Lösung zum Einsatz in reinen Microsoft Umgebungen. Microsoft reichert die Überwachung der Windows Plattform und der darauf laufenden Software um die eigene Erfahrung im Client-Management in Form von vorimplementierten Best-Practices und Workflows in das System an. Für heterogene Umgebungen mag dies ungeeignet sein, jedoch können sich in einer reinen Microsoft Umgebungen wesentliche Vorteile gegenüber einer einfachen Sicht auf die Landschaft ergeben. Ob MOM dieses Potential nutzen kann, bleibt abzuwarten. MOM bietet außerdem die Möglichkeit eigene Erweiterungen mit der .Net-Umgebung zu erstellen, um so kundenspezifische Software-Dienste einzubinden.

Zusätzlich zu den allgemeinen Lösungen für ein umfassendes System-Monitoring gibt es Speziallösungen auf dem Markt, die einen bestimmten spezialisierten Teil abdecken. Eine solche Software ist das weiter oben erwähnte Computer Center Management System(CCMS) der SAP AG. Eine andere Variante ist der System Insight Manager von HP, mit dem sich Komponenten unterhalb der Betriebssystemebene administrieren lassen. Der Insight Manager bietet zwar keine Performance-Daten, aber eine umfassende Überwachung aller einzeln erfassbaren Hardware-Komponenten für HP-Systeme (Lüfter, Festplatten, etc.). Zudem bietet er die Möglichkeit, Firmware-Stände zentral zu managen und zu aktualisieren. Vergleichbare Überwachungswerkzeuge mit Fokus auf die eigenen Hardwarekomponenten gibt es auch von anderen großen Hardwareherstellern.

Die Lizenzmodelle sind unterschiedlich und reichen vom Komplettpaket bis zur Knoten-basierten Lizenzierung. Allen Ansätzen gemein ist, dass für aktualisierte Software-Dienste in der Regel auch aktualisierte Überwachungssoftware zu beschaffen ist. Neben der klassischen Lizenzierung über den Kauf von Lizenzen und dem Abschluss eines Wartungsvertrages werden vermehrt Mietmodelle und „Software as a Service“-Lösungen angeboten.

### 4.2.2.6 Empfehlungen

Ein bedeutender Teil der Kosten für die Systemüberwachung entsteht dadurch, dass die Überwachung der zu überwachenden Systeme auf den jeweiligen Systemüberwachungswerkzeugen eingerichtet und aktuell gehalten werden muss. Neben Zeit erfordert dieses vor allem gute Kenntnisse in dem jeweiligen Werkzeug. Vor dem Hintergrund des Investitionsschutzes sind beim Wechsel des Systemüberwachungswerkzeuges neben möglichen Lizenz- und Wartungskosten insbesondere die Kosten und Aufwände für die Umstellung der bestehenden Lösung zu berücksichtigen. Dabei sind das in der Organisation vorhandene Wissen und der Umfang der bereits jetzt implementierten Lösung zu berücksichtigen. Ist eine Migration von einem Systemüberwachungswerkzeug auf ein anderes geplant, so ist zu klären, inwieweit die Möglichkeit besteht, Konfigurationen aus dem Bestandssystem zu übernehmen. Optimistische Zusagen kommerzieller Lösungsanbieter sollte man sich dabei vertraglich zusichern lassen.

Unverzichtbar für eine effektive Systemüberwachung ist, dass die Meldungen der Überwachungssysteme an einer zentralen Stelle zusammenlaufen. An dieser Stelle muss eine Gesamtsicht auf die überwachte Systemlandschaft möglich sein. Existieren mehrere Überwachungslösungen parallel, dann ist eine praktikable Option, das strategisch favorisierte System zum Master zu erklären, an das alle anderen Systeme ihre Zustände weitermelden, so dass in einem System die Gesamtsicht vorliegt. Bei diesem Vorgehen kann die wertvolle Überwachungsinfrastruktur der verschiedenen Systeme weiter genutzt werden, ohne den Vorteil einer zentralen Überwachung zu verlieren. Das Ablösen einzelner Überwachungssysteme ist bei diesem Ansatz ohne Zeit- oder Budgetdruck unkritisch möglich.

Alle kommerziellen Anbieter haben über die Systemüberwachung hinausgehende Lösungen im Angebot. Hat man bereits eine Configuration Management Database eines Herstellers in Betrieb, dann kann es aufgrund guter Integration vorteilhaft sein, auch die Systemüberwachung von diesem Anbieter zu beziehen. Dies gilt analog auch im OSS-Bereich. Ist beispielsweise OTRS[24] für das Incident- oder Changemanagement bereits in Betrieb, kann Nagios gut darin integriert werden.

Der Einsatz von Nagios für die Systemüberwachung ist aus technischer Sicht unkritisch und marktweit akzeptiert. Durch viele große Installationen, in denen mehrere tausend Überwachungsparameter erfolgreich überwacht werden, ist auch die Eignung für große Umgebungen nachgewiesen. Durch die gute Erweiterbarkeit mit Konnektoren kann mit dieser freien Software nahezu jede Überwachung durchgeführt werden. Dies setzt jedoch ggf. die Bereitschaft voraus, sich in der Community zu bewegen und verfügbare Konnektoren zu nutzen oder eigene zu entwickeln.

Um abzusichern, dass durch Migrationsprojekte oder Softwareeinführungsprojekte zu betreibende neue System- und Anwendungslandschaften entsprechend überwacht werden können, sollte der jeweilige Systemüberwachungsstandard organisationsweit bekannt sein und die daraus resultierenden Anforderungen in den Pflichtenheften hinterlegt werden.

#### 4.2.2.7 Ausblick

Die in diesem Kapitel beschriebene Überwachung konzentriert sich auf Hardware, Software und Applikationen. Diese technische Sicht wird in Zukunft nicht mehr ausreichend sein. Vielmehr werden die Verfügbarkeit von Fachverfahren und Geschäftsprozessen sowie deren Antwortzeiten wesentliche Kriterien sein, an denen sich eine IT messen lassen muss.

Die Überwachung von Fachverfahren und Geschäftsprozessen wird nicht alternativ zu der bisherigen Überwachung, sondern ergänzend zu dieser erfolgen. Die großen Systemüberwachungslösungen – auch im Open Source Bereich – haben diese Anforderungen erkannt und bieten Erweiterungen und Module, die diese Anforderungen bereits teilweise erfüllen. Die Voraussetzung für eine effektive Nutzung ist, dass die zu überwachenden Prozesse über definierte Schnittstellen eine solche Überwachung ermöglichen. Bei der Einführung von neuen Anwendungssystemen und Verfahren sollten diese Schnittstellen heute gleich definiert werden.

[24] http://www.otrs.org

### 4.2.3 Authentisierungs- und Verzeichnisdienste

#### 4.2.3.1 Einleitung

Verzeichnisdienste ermöglichen in Netzwerken den Zugriff auf eine Sammlung bestimmter Daten, einer Art Telefonbuch, das nach Typen und Bereichen sortierte Informationen über Objekte enthält. Meist sind dies benutzer- oder gerätespezifische Daten, die von verschiedenen Anwendungen verwendet werden. Die zentrale Verwaltung und Speicherung hat den Vorteil, dass die Daten konsistent sind und sich eine Änderung an einer Stelle auch auf alle anderen verbundenen Anwendungen auswirkt. Angesichts immer umfangreicherer, verteilter IT-Infrastrukturen kommt deren möglichst einfacher Verwaltung, der Informations-Konsistenz, -Kontrolle und Übersichtlichkeit zentrale Bedeutung zu. Verzeichnisdienste sind dafür elementare Hilfsmittel, weil sich damit Netzwerke kosteneffektiv und mit vergleichsweise wenig Aufwand in einheitlicher Art und Weise verwalten lassen.

Die meisten Verbindungen zu Verzeichnisdiensten sind lesender Art; schreibende Zugriffe für das Hinzufügen, Ändern oder Löschen gespeicherter Informationen sind angesichts der Langlebigkeit der hinterlegten Informationen vergleichsweise selten. Dadurch und durch die einfachen Datenstrukturen sind schnelle Zugriffszeiten die Regel. Häufig werden Verzeichnisdienste für die Authentisierung der Benutzer an Systemen innerhalb einer IT-Infrastruktur verwendet. Hier sorgt die zentrale Speicherung beispielsweise dafür, dass der Benutzer sich an allen angeschlossenen Clients mit dem selben Passwort und Benutzernamen für verschiedene Anwendungen anmelden kann. Analog können systemweit zu Geräten Informationen wie Standort oder druckbare Seiten pro Minute hinterlegt und abgefragt werden.

Für den Zugriff auf die hinterlegten Informationen eines Verzeichnisses werden spezielle Netzwerkprotokolle verwendet. 1988 wurde der auf dem ISO/OSI-Modell basierende Standard ISO/ITU X.500(1988) entwickelt, der u.a. das Directory Access Protocoll (DAP) für Client-Zugriffe auf Verzeichnisdienste vorsieht; daneben sind weitere Protokolle definiert für Abfragen zwischen X.500-Servern und für Replikationen. Angesichts der Komplexität des Standards und insbesondere des DAP wurde bereits wenige Jahre später eine vereinfachte (lightweight) Zugriffsvariante namens LDAP entwickelt, die zunächst als Mittler zwischen den Clients und dem DAP für den Zugriff auf den X.500-Server eingesetzt wurde.

LDAP beschränkt sich auf das TCP/IP-Protokoll und weist gegenüber der X.500-Schnittstelle X/Open XDS deutliche Vereinfachungen auf. Neben auf das Notwendige beschränkter Funktionalität zählt dazu beispielsweise die Festlegung auf (ggf. verschlüsselte) einfache Zeichenketten für die Formulierung von Anfragen und Antworten. Diese Vereinfachungen führten zu einer raschen Verbreitung von LDAP als Zugriffsprotokoll. Als Folge der Verbreitung führten die Hersteller von X.500-Servern Erweiterungen ein, die das bis dahin notwendige Übersetzen von LDAP zu DAP erübrigten. Zudem entstanden reine LDAP-Server, die lediglich die zur Implementierung des Protokolls benötigte Funktionalität ohne die sonstigen X.500-Spezifika aufweisen. LDAP liegt derzeit in Version 3 (LDAPv3) vor und ist über die IETF in den RFCs 4510[25] bis 4519 offen standardisiert.

#### 4.2.3.2 Kriterienkatalog

Ein Verzeichnisdienst hat in erster Linie die Aufgabe, beliebig viele Anwendungen mit Daten aus dem zentralen Verzeichnis zu versorgen. Dabei gibt es verschiedene Möglichkeiten, wie Anwendungen an einen Verzeichnisdienst angebunden werden können (s.o.). Am weitesten verbreitet ist das LDAP-Protokoll, auf das auch Microsofts AD zurückgreift, um Anwendungen zu unterstützen, die nicht direkt mit dem AD sprechen können.

Ein Verzeichnis wird anhand eines Schemas strukturiert. Dieses sollte **Container für alle wesentlichen Komponenten einer IT-Landschaft** aufweisen, insbesondere für Benutzer, Benutzergruppen, Arbeitsplatzrechner, Server und Drucker. Für diese Komponenten müssen **Eingenschaften und Regeln** definiert werden können, die festlegen, welche Komponente welche Rechte an einer anderen Komponente besitzt. Mit Hilfe von spezifischen Konstrukten und **Organisationseinheiten** sollte eine **Hierarchie** auf-

[25] http://tools.ietf.org/html/rfc4510

gebaut werden können, die die reale IT-Landschaft unter organisatorischen und räumlichen Gesichtspunkten möglichst genau nachbildet.

Verzeichnisdienste werden vielfach zur Authentisierung und Autorisierung von Anwendern genutzt und müssen zu diesen folglich viele Eigenschaften verwalten. Deren leichte und übersichtliche Administration ist für die Systembetreuer wesentlich und wird daher zusammen mit sonstigen **allgemeinen Eigenschaften** der Alternativen und deren **Aufbau** beleuchtet.

#### 4.2.3.3 Methodik

Zunächst ist festzustellen, welche Verzeichnisdienste derzeit eingesetzt werden. Weiterhin muss geprüft werden, welche Daten im Verzeichnis enthalten und wie sie organisiert sind (Schema). Zudem ist zu ermitteln, in welcher Form die hinterlegten Informationen exportiert werden können und ob das Schema in der exportierten Form erhalten bleibt. Hinsichtlich der Verwendung der Verzeichnisdienste ist festzustellen, welche Anwendungen derzeit darauf zugreifen, welche Daten dabei abgerufen werden und in welcher Form die Anbindung der Anwendungen an die Verzeichnisdienste stattfindet. Diese Informationen sollten über die Systemadministration beschafft werden können.

Das derzeitige Schema ist auf aktuelle Strukturen und Hierarchien sowie auf die Vollständigkeit der abgebildeten Bereiche und Objektarten zu prüfen. Dabei sind Anforderungen an die Replizierung oder Aufteilung des Datenbestands zu beachten. Sofern eine Überarbeitung des Schemas notwendig ist, sollte dies vor der eigentlichen Migration geplant und modelliert werden. Die konzipierten Änderungen sind während oder unmittelbar nach der Migration des Verzeichnisdiensts auf der Basis des künftig eingesetzten Produkts umzusetzen. Zudem ist zu prüfen, welche der bisherigen Anwendungen in einer erweiterten Form Informationen von einem Verzeichnisdienst abfragen sollen und welche bisher noch nicht angeschlossenen Anwendungen zusätzlich einen Zugriff darauf benötigen.

#### 4.2.3.4 Betrachtete Alternativen

Mangels vergleichbarer Absatzzahlen oder belastbarer Erhebungen kann die tatsächliche Verbreitung einzelner Produkte dieses Marktsegments nur geschätzt werden. Auf dieser Basis werden folgende Alternativen nachfolgend näher betrachtet:

- **Microsoft Active Directory** als Marktführer,
- **Samba 4** als Nachfolger des in Behörden verbreiteten Samba 3 sowie
- **OpenLDAP** als weit verbreiteter OSS-Alternative.

#### 4.2.3.5 Bewertung

##### 4.2.3.5.1 Active Directory (AD)

Active Directory ist ein von Microsoft entwickelter Verzeichnisdienst für Windows Server. Ab der Version Windows Server 2008 umfasst Active Directory mehrere Domain Services (ADDS), die unterschiedliche Funktionalitäten zusammenbringen. Active Directory verwaltet die verschiedenen Objekte, die in einer IT-Landschaft relevant sind. Dies sind Benutzer, Gruppen, Computer, Drucker, Server, Dienste und andere Geräte und deren spezifische Einstellungen. Dadurch wird die Möglichkeit geschaffen, ein Netzwerk entsprechend der realen Struktur eines Unternehmens oder auch seiner räumlichen Verteilung zu gliedern. Die Verwaltung erfolgt am zentralen Datensatz und kann nur an den dafür vorgesehenen Stellen von den berechtigten Personen durchgeführt werden. Mit Windows Server 2008 und der Einführung des ADDS sind fünf verschiedene Serverrollen unter dem Dach des Active Directory zusammengefasst:

**Active Directory Domain Services (ADDS)** Das ursprüngliche ActiveDirctory ist der zentrale Punkt des Verzeichnisdienstes und beherbergt die Ressourcen- und Domänenverwaltung.

**Active Directory Lightweight Directory Services (ADLDS)** Bietet funktionell eingeschränkte Active Directory-Dienste für Funktionen und Anwendungen an, die LDAP-konforme Informationen benötigen. Dadurch können auch diese an das Active Directory angebunden werden.

**Active Directory Rights Management Services (ADRMS)** Das Sicherheitsmodul des Pakets. Es schützt vor unbefugtem Zugriff, indem es verschiedene kryptographische Methoden bereitstellt, mit denen die Daten gesichert werden.

**Active Directory Federation Services (ADFS)** Dieser Dienst ist für die webbasierte Authentifizierung außerhalb der ADDS-Bereiche zuständig.

**Active Directory Certificate Services (ADCS)** Die Komponente für die Zertifikatsverwaltung und Public-Key Infrastruktur.

Diese Rollen greifen in ihrer Funktionalität auf verschiedene Hauptkomponenten eines Active Directory-Servers zurück, die wiederum die Funktionsweise erst ermöglichen. Zum einen ist dies ein LDAP-Verzeichnis, in dem von AD Informationen über Benutzer und Komponenten, deren Gruppenzugehörigkeit und Rechte sowie andere zugehörige Daten gespeichert und miteinander verknüpft werden. Neben den Benutzerdaten wie zum Beispiel dem Passwort werden unter anderem auch Zertifikate eines Rechners in diesem Verzeichnis gespeichert. Diese Daten können über das LDAP-Protokoll mit der entsprechenden Syntax abgerufen werden. Über das CIFS wird die Ablage und Verwaltung von sowie der Zugriff auf Daten realisiert. Aufgrund des standardisierten Protokolls stellt es auch eine Möglichkeit zur Anbindung an das Internet dar.

Zum Auffinden der einzelnen Computersysteme und Dienstinformationen wird im Gegensatz zu früheren Windows-Versionen, die NetBIOS zur Namensauflösung verwendet haben, DNS genutzt. Ältere Windows-Systeme der 2000er oder XP-Generation können bei entsprechender Konfiguration aber auch im Active Directory mit Hilfe von NetBIOS Ressourcen im Netzwerk ausfindig machen, eine Abwärtskompatibilität ist in diesem Punkt vorhanden. Die letzte Hauptkomponente ist Kerberos zur Authentifizierung und für den Zugriff auf bestimmte Dienste im Netzwerk. Die Passworteingabe ist dabei nur einmal nötig, die Autorisierung gegenüber anderen Diensten läuft auf Basis des Kerberos-Tickets im Hintergrund ab.

Die verwalteten Ressourcen werden im AD objektbasiert und hierarchisch strukturiert. Eigenschaften können als Attribute zugeordnet und an untergeordnete Objekte vererbt werden. Dadurch können Netzwerke und IT-Landschaften nach logischen Gesichtspunkten gruppiert und entsprechend der realen Struktur organisiert werden. In der Gesamtstruktur, die im AD-Jargon als Wald (forest) bezeichnet wird, werden alle Objekte und deren Attribute abgelegt. Innerhalb der Gesamtstruktur existieren mehrere Bäume (trees), die transitiv verknüpft sind und gleichzeitig die wiederum transitiv verknüpften Domänen verwalten. Damit die Objekte innerhalb des Waldes gruppiert und geordnet werden können, gibt es Containerobjekte – die sogenannten Organisationseinheiten (Organisational Unit – OU). Durch geschickte Verschachtelung und Verknüpfung kann mit Hilfe der OU die Netzwerk- oder Organisationsstruktur einer Behörde oder einer Abteilung nachgebildet werden. Aufgrund der umfangreichen Möglichkeiten zur Organisation der Daten innerhalb des Verzeichnisdienstes ist eine sorgfältige Planung bereits vor dem Aufsetzen einer solchen Verzeichnisstruktur unumgänglich. Eine Hilfe für den Systemadministrator bieten vorkonfigurierte oder selbst definierte Schemata als Muster für Active Directory-Einträge eines bestimmten Typs. Sie definieren deren Objekttypen, die Attribute und die Attributsyntax.

Zur Speicherung der Daten verwendet Active Directory eine relationale, transaktionsorientierte Jet (Blue)-Datenbank, die von Microsoft auch für Exchange eingesetzt wird. Die Active Directory-Datenbank ist auf eine Größe von 17 Terabytes und 10 Millionen Objekte pro Domäne begrenzt. Diese Grenze ist allerdings eher theoretischer Natur, da nicht mehr als eine Million Objekte pro Domäne empfohlen werden. Die Datenbankdatei NTDS.DIT enthält drei Haupttabellen: die „schema table“ zur Speicherung der Schemata, die „link table“ zur Speicherung der Objekt-Struktur und die „data table“ zur Speicherung der Daten. Für das Ordnen der Daten nach dem vorgegebenen Schema ist eine Extensible Storage Engine (ESE) verantwortlich, die die nach einem relationalen Modell abgespeicherten Active-Directory-Daten in einem hierarchischen Modell anordnet.

#### 4.2.3.5.2 OpenLDAP

OpenLDAP ist eine Open-Source-Implementierung des LDAP-Protokolls und der entsprechenden Server-Funktionalität und Bestandteil der meisten Linux-Distributionen, läuft aber auch unter Windows und MacOS. Damit ist dieses Produkt ein sogenannter Stand-alone LDAP-Server, also ein Verzeichnisdienst, der Daten und Komponenten verwaltet und Clients mittels LDAP zur Verfügung stellt. OpenLDAP ist als freie Software unter der der BSD-Lizenz ähnlichen OpenLDAP Public License veröffentlicht und stellt die Referenzimplementierung des LDAP-Protokolls dar. Schemadateien werden daher besonders sorgfältig auf Protokollkonformität geprüft, was zu gelegentlichen Fehlermeldungen beim Import solcher Dateien von Directory Server Agents anderer Hersteller führt. OpenLDAP ist ein leistungsfähiges und gut skalierendes Produkt und besteht nicht nur aus dem Verzeichnisdienst, sondern umfasst auch noch andere Werkzeuge und zur Konfiguration benötigte Bibliotheken. Im einzelnen sind dies:

**slapd** Der Daemon, der den Stand-alone Verzeichnisdienst bereitstellt.

**slurpd** Stand-alone Update Replication Daemon.

**overlays** Ermöglichen erweiterte Operationen.

**syncrepl** Sorgt für Synchronisation und Replikation gemäß RFC 4533.

**Bibliotheken und Werkzeuge** Stellen das LDAP-Protokoll bereit und bieten Hilfsmittel und Beispiele, die den Betrieb vereinfachen.

Daten werden objektorientiert vorgehalten. Eine Objektklasse beschreibt eine spezifische Sammlung von Attributen, auf deren Basis einzelne Verzeichniseinträge (Objekte) gespeichert und gelesen werden können. Vordefinierte Objektklassen sind für Lokationen, Organisationen, Firmen, Personen und Gruppen vorhanden. Konzeptuell orientiert sich OpenLDAP am Aufbau des Domain Name Service. Oft gewählte Attribute im Standard-LDAP-Schema sind Common Name (CN), Organisational Unit (OU) und Country (C). Benutzer- oder Organisationsdaten lassen sich über Dateien im Lightweight Data Interchange Format (LDIF) in das LDAP-Schema einpflegen. LDIF kann auch für viele andere Zwecke verwendet werden, beispielsweise für den Export eines bestehenden LDAP-Baums.

#### 4.2.3.5.3 Samba 4

Samba entstand 1992 aus dem Anspruch, den Datenaustausch zwischen SunOS und DOS-Rechnern ohne das auf Letzteren nicht unterstützte Network File System (NFS) zu ermöglichen. Mit dem Aufkommen von Linux und der Portierung von Samba auf diese Plattform wurde das Vorhaben erweitert um die gemeinsame Nutzung von Dateien, Verzeichnissen und Druckern durch Linux- und Windows-Clients. Samba implementierte hierfür eine beträchtliche Anzahl an Protokollen und Services, u.a. NetBIOS, WINS, SMB und CIFS. Gemeinsam genutzte Netz-Ressourcen auf der Basis von Samba 3 sind heute weit verbreitet und wie angestrebt von Windows- und Linux-Clients gleichermaßen nutzbar. Die Zugriffsrechte können mittels Access Control Lists (ACLs) fein differenziert und beliebig gesetzt werden.

Samba 4 soll als Nachfolger von Version 3 etliche Verbesserungen und neue Features bringen und unter anderem auch als vollständig Active Directory-kompatibler Domain Controller fungieren können (Bar05). Das derzeit freigegebene Samba 3 hingegen arbeitet lediglich als Partner eines zusätzlichen Active Directory, kann aber dessen Dienste nicht selbst bereitstellen. Dies hat zur Folge, dass man beim Einsatz von Samba 3 einen zusätzlichen Windows Server mit AD betreiben muss, wenn man Systeme in einem Netzwerk zu einem Verbund zusammenschließen und Benutzer zentral verwalten will (Sie10).

Samba 4 befindet sich derzeit laut Samba-Team noch in der Entwicklung; ein konkreter Termin für ein erstes Stable-Release von Samba 4 ist nicht bekannt[26]. Allerdings setzt Univention für die kommende Version 3.0 seines Corporate Server UCS bereits auf Samba 4 auf[27] und stellt entsprechen-

[26] http://wiki.samba.org/index.php/Samba4, abgerufen: 27.10.2011

[27] http://www.univention.de/univention/news/aktuell/univention-veroeffentlicht-prototyp-mit-samba4/, abgerufen: 27.10.2011

de Testversionen bereit. Bereits in Samba 4 implementierte Verbesserungen gegenüber der Vorgängerversion sind ein integrierter LDAP-Server mit AD-Semantik, ein DNS-Server (Bind9) für den AD-DNS-Support sowie Kerberos. Die ebenfalls weitgehend implementierten Erweiterungen für die Active Directory-Funktionalität und dem Microsoft-Verzeichnisdienst entsprechende Datenstrukturen machen Samba 4 mit dessen Freigabe zu einer ernstzunehmenden Open-Source Alternative zu AD. Daher sollten der Entwicklungsstatus von Samba 4 und des UCS im Auge behalten werden. Mit Hilfe einer von Samba bereitgestellten Anleitung[28] kann mit der aktuellen Alpha-Version ein Domänen-Controller testweise eingerichtet werden.

#### 4.2.3.6 Empfehlungen

Die Datenstrukturen innerhalb der betrachteten Verzeichnisse sind ähnlich aufgebaut, so dass sich hieraus für keine der beiden Alternativen – Samba 4 sei hier außen vor – Vorteile ergeben. Einträge werden mit Containern gegliedert, einer Objektklasse zugeordnet und nach einem vorher definierten Schema eingepflegt. Standardobjektklassen sind zum Beispiel *Organisation*, *organisationalUnit*, *Person* oder *Country*. Eine eindeutige und allgemeingültige Empfehlung für einen konkreten Verzeichnisdienste ist derzeit nicht sinnvoll, da die Stärken und Schwächen der Alternativen stark von ihrer Umgebung und der prinzipiellen Ausrichtung der zu verwaltenden Systeme abhängen.

In reinen Windows-Umgebungen ist derzeit der Einsatz von Active Directory als Verzeichnisdienst sinnvoll, weil AD exakt darauf zugeschnitten ist und alle nötigen Funktionen zur Verwaltung von Windows-Domänen bereitstellt. Beim vermehrten Einsatz von Linux- oder MacOS-basierten Systemen gilt dies nicht mehr uneingeschränkt, da solche Systeme nur einen kleinen Teil der AD-Funktionalitäten verwenden können. Hier empfiehlt sich die Einrichtung eines LDAP-Servers wie OpenLDAP, der alle für einen Verzeichnisdienst relevanten Funktionen bietet und schnell und einfach an jedes System angebunden werden kann. Reine LDAP-Server sind zudem sparsam im Verbrauch von Systemressourcen, skalieren gut und sind in verschiedenen Varianten auf allen Plattformen verfügbar. In heterogenen Infrastrukturen ist derzeit ein Parallelbetrieb von LDAP-Server und AD sinnvoll, da sich beide nicht gegenseitig stören und jede Ressource sich mit dem jeweils passenden Verzeichnisdienst verbinden kann. Zu beachten ist hierbei aber eine konsistente Datenhaltung beider Server. Diese Empfehlungen gelten bis zur Veröffentlichung einer stabilen Version von Samba 4, welches die Vorteile der beiden anderen Produkte vereint und daher als Alternative zu AD genau geprüft werden sollte.

Unabhängig von einer Migration des Verzeichnisdiensts sollten die im derzeitigen Verzeichnis hinterlegten Daten und Strukturen nach größeren Änderungen oder Erweiterungen der Umgebung auf Aktualität, Übersichtlichkeit und Vollständigkeit geprüft werden. Entsprechende Korrekturen können ggf. noch im bestehenden Verzeichnisdienst umgesetzt werden, erleichtern dadurch den Systembetrieb und ebnen einer anstehenden Migration den Weg.

#### 4.2.3.7 Migrations-Checkliste

Die nachfolgende Checkliste stellt sicher, dass alle relevanten Aspekte bei der Migration von Verzeichnisdiensten berücksichtigt werden. Die unter den Arbeitsschritten stehenden Informationen zeigen, wie die Bewertungskriterien konkretisiert werden können.

##### 4.2.3.7.1 Ist-Analyse

1. Verzeichnisdienst(e) identifizieren
2. Genutzte Funktionalität, Probleme und denkbare Erweiterungen feststellen
3. Vorhandene Daten und Struktur des Verzeichnisses analysieren
4. Heterogenität der IT-Landschaft innerhalb der Domäne prüfen

[28] http://wiki.samba.org/index.php/Samba4/HOWTO

5. Den Verzeichnisdienst nutzende Anwendungen erfassen

#### 4.2.3.7.2 Ist-Analyse auswerten

1. Liste eingesetzter Verzeichnisdienste
2. Liste der diese nutzenden Anwendungen
3. Möglichkeiten und Formate für Daten-Im- und -Export
4. Priorisierung der Anforderungen
5. Konsolidieren der gewonnenen Erkenntnisse

#### 4.2.3.7.3 Soll-Konzeption durchführen

1. Modellierung der künftigen Verzeichnisstruktur
2. Festlegen der zu verwendenden Standards und Protokolle
3. Festlegen der anzubindenden Anwendungen
4. Festlegen der Domänenspezifika und Ausnahmen

#### 4.2.3.7.4 Bewertung und Entscheidung

1. Vorauswahl der Prüfkandidaten
2. Berücksichtigung der Systemplattformen
3. Abgleich der Anforderungen an die Basisfunktionalität

### 4.2.4 Groupware

#### 4.2.4.1 Einleitung

Eine Groupware ist eine Software, die die Zusammenarbeit in einer Gruppe über zeitliche und/oder räumliche Distanz hinweg unterstützt und Schnittstellen für eine geteilte Arbeitsumgebung bietet. Groupware-Lösungen werden eingesetzt, um die Kommunikation und Planung innerhalb einer Personengruppe zu vereinfachen. Zu diesem Zweck werden verschiedene Informationen und Daten auf dem Groupware-Server gespeichert und über ein Webinterface oder über einen Personal Information Manager abgerufen und gepflegt.

Dabei dient ein Groupware-Server als zentrales E-Mail- und Kommunikationssystem und verwaltet zudem Termine, Adressen und Kontakte, Aufgaben sowie Notizen. Einige solche Lösungen bieten auch die Möglichkeit, bestimmte Verzeichnisse auf dem Server mehreren Benutzern gemeinsam zur Verfügung zu stellen. Durch die zentrale, serverseitige Speicherung dieser Daten kann je nach Einstellung und Kategorie mit feingranularen Rechten für jede Ressource gesteuert werden, welche Daten welchen Benutzern oder Benutzergruppen zugänglich sind. Die zentrale Speicherung verhindert außerdem Inkonsistenzen und Missverständnisse und vereinfacht die Koordination von Terminen innerhalb einer großen Anzahl von Personen.

Zum faktischen Weltmarktführer Microsoft Exchange Server gibt es viele alternative Groupware-Lösungen. Der Migrationsleitfaden betrachtet zwei davon (siehe Abschnitt 4.2.4.4 und folgende). Mit Lotus Notes, Zimbra, eGroupware, Tine2.0, Horde und Open-Xchange seien hier beispielhaft weitere Produkte erwähnt, die ebenfalls einen näheren Blick lohnen.

#### 4.2.4.2 Kriterienkatalog

Zentrale Aspekte eines Groupware-Servers sind aufgrund der verschiedenen Bereiche, in denen er eingesetzt wird, vielfältig. Mindestanforderungen an die **Funktionalität** eines solchen Servers sind die in der Einleitung bereits angesprochenen Aufgaben E-Mail, Kalender, Kontaktverwaltung mittels Adressbuch und eine Aufgabenliste. Diese sind auch gleichzeitig die Grundfunktionalitäten eines PIM. Des Weiteren sollte der Zugriff auf die verwalteten Daten und E-Mails über ein Webinterface möglich sein, damit Benutzer mobil und ohne speziell installierten Client auf die Groupware zugreifen können. Manche Anbieter stellen eigens entwickelte Clients zur Verfügung, die im Gegensatz zu anderen PIM eine bessere, reibungslosere Anbindung an den Server gewährleisten sollen.

Nicht jede Groupware kann auf jedem Betriebssystem installiert werden. Die diesbezüglichen **Anforderungen** der betrachteten Lösungen müssen daher untersucht werden. Während Microsoft seine Groupware Exchange nur für Windows Server zur Verfügung stellt, der Anteil von unixoiden Betriebssystemen in der Serverlandschaft aber enorm ist, muss eine entsprechende Betrachtung der **Kompatibilität** in die Bewertung einfließen. Hardwareanforderungen an den Server werden in diesem Zusammenhang ebenfalls betrachtet.

Nur wenige Anbieter stellen ihre Groupware als OSS zur Verfügung. Ein häufiges Modell ist hingegen die Bereitstellung der Groupware als Open-Core-Software, bei der nur Teile der Funktionalität frei zur Verfügung gestellt und durch proprietäre, kostenpflichtige Add-Ons ergänzt wird. Weitere Alternativen werden vollständig unter proprietären Lizenzen angeboten. Die für die jeweilige Groupware angebotenen Arten der **Lizenzierung** und damit der **Kosten** sind folglich weitere Kriterien für die Analyse.

Der anzusetzende **Wartungsaufwand** ist für den IT-Betrieb relevant und wird ebenfalls bewertet. Er umfasst das Einspielen von Updates, Produktaktualisierungen, Konfigurationen, das Einrichten neuer Benutzer, die Archivierung alter Daten und weitere ähnliche Tätigkeiten.

Weitere Kriterien betreffen das Zusammenspiel mit Anwenderprogrammen, insbesondere mit PIM. Es ist zu prüfen, wie viele solcher Clients sich gleichzeitig mit einer Groupware-Instanz **verbinden** können und ob es hierbei Einschränkungen durch **Lizenzen** oder hohe **Hardwareanforderungen** gibt. Ebenfalls zu prüfen ist, über welche **Protokolle** die Kommunikation mit den Clients stattfinden, wie die **Synchronisation** mit Mobilgeräten realisiert und wie Datenhaltung, -zugriff und -transport **abgesichert** sind.

Schließlich werden die **Erweiterbarkeit** der Serverfunktionalität durch Plug-Ins oder zusätzlich zu installierende Software und eventuelle **Einschränkungen** durch bekannte Probleme oder nicht unterstütze Formate und Protokolle bewertet.

#### 4.2.4.3 Methodik

In einem ersten Schritt wird der Ist-Zustand ermittelt. Dies beinhaltet sowohl die von den Benutzern eingesetzten Clients (PIM, Webinterfaces, Mobilgeräte), die verwendeten Server- und Client-seitigen Betriebssysteme, die innerhalb der Groupware benutzten Funktionen sowie die Struktur der Serverlandschaft. Insbesondere die Anzahl und Heterogenität der mit der Groupware kommunizierenden Clients sind für die Bewertung relevant. Sollten diese Informationen nicht durch Richtlinien festgelegt sein, sollten die Benutzer und die verantwortlichen Systemadministratoren befragt werden.

Es ist zu klären, inwieweit derzeit Clients auf die Groupware abgestimmt werden müssen, um eine Synchronisation zu ermöglichen oder den vollen Umfang der Groupware nutzen zu können. Gerade durch den Boom mobiler Geräte wie Smartphones und Tablets[29] sind neue Anforderungen bezüglich der Synchronisation entstanden, die es zu beachten gilt. Festzustellen sind die verwendeten Protokolle und Formate für die Synchronisation, den E-Mail-Zugriff sowie den Zugriff auf Kontakt- und Kalenderdaten. Zudem sind damit verbundene Probleme aufzudecken.

Bei der Erarbeitung des Soll-Zustands müssen die derzeit verwendeten Funktionalitäten als Mindestanforderung berücksichtigt werden. Zudem muss geprüft werden, in wie weit Abhängigkeiten zu vorhandenen und künftigen Client-Systemen bestehen, da die künftige Groupware-Lösung eine Mindest-Kompatibilität zu den Nutzersystemen aufweisen muss. Zu berücksichtigen sind ggf. vorgegebene Server-Plattformen, einzubindende Infrastruktur-Systeme wie Verzeichnisdienste, Betriebsanforderungen hinsichtlich Verfügbarkeit und Wartungsfenstern, vorgegebene Hardware oder vorhandene Rahmenverträge für den Bezug von Software oder Dienstleistungen.

#### 4.2.4.4 Betrachtete Alternativen

Mangels vergleichbarer Absatzzahlen oder belastbarer Erhebungen kann die tatsächliche Verbreitung einzelner Produkte dieses Marktsegments nur geschätzt werden. Auf dieser Basis werden folgende Alternativen nachfolgend näher betrachtet:

- **Microsoft Exchange Server** als Marktführer,
- **Zarafa**[30] als in Behörden verbreitete Alternative zum Microsoft Exchange Server und
- **Kolab**[31] als verbreitetes OSS-Produkt.

#### 4.2.4.5 Bewertung

##### 4.2.4.5.1 Microsoft Exchange

Der Exchange Server ist ein Groupware- und Nachrichtensystem des Unternehmens Microsoft und wurde 1996 eingeführt. Ursprünglich als reiner E-Mail-Server konzipiert, kamen mit der Zeit immer mehr Funktionen dazu, die Exchange zur vollständigen Groupware-Lösung werden ließen. Der Exchange Server bietet mit den Komponenten E-Mail-Server, Terminkalender, Aufgabenliste und Adressbuch alle Bestandteile der o.g. Grundfunktionalität. Des weiteren können auf dem Exchange Server Notizen und Dokumente zentral verwaltet und innerhalb von definierten Benutzergruppen bereitgestellt werden.

Jede Komponente kann umfangreich per grafischem Assistenten konfiguriert werden. So hat der Benutzer im E-Mail-Bereich die Möglichkeit, Nachrichtenfilter zu konfigurieren, Abwesenheitsbenachrichtigungen einzustellen und auf dem Server eine eigene Verzeichnisstruktur zum Sortieren von Mails anzu-

[29] Als Tablets werden Finger- oder Stift-gesteuerte Mobilgeräte mit mittleren Bildschirmgrößen wie das Apple iPad bezeichnet.
[30] http://www.zarafa.com
[31] http://www.kolab.org

legen. Das Archivieren von E-Mails wird durch eine Backup-Funktion des Servers unterstützt. Der Kalender bietet die üblichen Funktionen: Neben dem Anlegen, Verwalten und Teilen von Terminen können auch Ressourcen (Räume, Beamer, etc.) angelegt und verwaltet werden, die dann im Zusammenhang mit Terminen oder einzeln gebucht werden können. Eine spezielle Ansicht, in der die Termine mehrerer Benutzer über einen bestimmten Zeitraum angezeigt werden können, vereinfacht das Finden von passenden Zeiten für Termine mit mehreren Teilnehmern. Im Adressbuch können persönliche Kontakte mit verschiedenen, vorher angelegten Benutzergruppen geteilt und globale Adressbücher verwaltet werden.

Der Exchange Server findet vor allem in von Microsoft-Produkten geprägten Infrastrukturen Verwendung und eignet sich für alle Größen von Netzwerken. Er wird in einer Standard- und einer Enterprise-Version vertrieben, die sich im Umfang ihrer Konfigurationsmöglichkeiten unterscheiden. Die beiden Lizenzierungsvarianten zielen auf Größe und Umfang des Einsatzes ab. Die Standard-Version ist auf kleine und mittelgroße Benutzergruppen ausgerichtet und bietet die volle Bandbreite an Grundfunktionalitäten bei eingeschränkter Konfigurierbarkeit bezüglich Speichergruppen, Datenbankgröße und Clustering. In der Enterprise-Version wird die Anbindung einer größeren Anzahl an Benutzern ermöglicht, indem größere Datenbanken angebunden und mehrere Speichergruppen definiert werden können. Zusätzlich können Enterprise-Exchange-Server als Cluster betrieben werden, wodurch Ausfallsicherheit und Performance gesteigert werden können. Allerdings fallen je nach Lizenzierungsvariante und Anzahl der Benutzer erhebliche Kosten an.

Mit dem Outlook Web Access (OWA) stellt Microsoft eine Webschnittstelle bereit, mit der über HTTP oder HTTPS per Browser direkt auf alle Grundfunktionalität von Exchange zugegriffen werden kann. Da diese Art des Zugriffs funktional nahezu identisch mit dem Zugriff per Outlook-Client und ihm auch optisch nachempfunden ist, wird auch deren Konfiguration und Verwaltung durch OWA unterstützt. Nachteilig dabei ist, dass trotz Verwendung des offenen HTTP(S)-Standards die vollständige Funktionalität des OWA nur dem proprietären Internet Explorer aus demselben Hause vorbehalten ist. Alle anderen Browser müssen mit der eingeschränkten Variante Outlook Web Access Light Vorlieb nehmen, die gegenüber dem vollständigen OWA in Puncto Konfigurationsmöglichkeiten, Bedienbarkeit und Funktionalität deutlich abgespeckt ist.

Die bevorzugte Art des Exchange Servers, mit seinen Clients zu kommunizieren, ist die von Microsoft entwickelte MAPI-Schnittstelle. Der volle Komfort und Funktionsumfang von Exchange kann nur durch deren Verwendung gewährleistet werden. Dies zielt auf eine enge Bindung an Outlook als diese unterstützenden Client ab. Der E-Mail-Verkehr wird bei der Verwendung von MAPI über die „Microsoft-Direct-Push“-Strategie realisiert. Für die Synchronisation mit mobilen Clients greift Exchange auf den eigenen, proprietären Standard ActiveSync zurück. Die offenen Protokolle POP3 und IMAP werden serverseitig nicht vollständig unterstützt. Außerdem muss IMAP beispielsweise extra auf dem Server freigeschaltet werden, in der Grundkonfiguration ist diese Art des Zugriffs deaktiviert und somit nicht möglich.

Die Sicherheit der Verbindungen wird durch eine Zertifikats-basierte Authentifizierung gewährleistet, SSL-/TLS-Connections sind möglich. Das Versenden von mit S/MIME verschlüsselten E-Mails stellt kein Problem dar. Die üblichen Methoden, um Benutzer vor unerwünschten E-Mails zu schützen, sind vorhanden. Exchange bietet hier einen intelligenten Anti-Spam-Filter und implementiert globales Black- und Whitelisting. Ein Interface zur Verwendung von Virenscannern von Drittanbietern ist vorhanden. Darüber hinaus ist die Erweiterbarkeit von Exchange über die mitgelieferten Komponenten hinaus nur in sehr begrenztem Umfang möglich.

Der Exchange Server benötigt eine Windows Server als Plattform, ist nur als 64-Bit-Version erhältlich und hat im Vergleich zu den anderen untersuchten Produkten die mit Abstand höchsten Hardwareanforderungen. Die maximale Speicherkapazität pro User ist durch Exchange auf ein Fixum beschränkt. Diese Menge hängt von der maximalen Größe der Datenbanken ab, die ihrerseits abhängig von der Lizenzierungsvariante ist. Besonders bei vielen Benutzern mit großen Postfächern kann dies zu Problemen führen, die sich im schlechtesten Falle nur durch das Aufstellen weiterer Server samt zusätzlichen Lizenzkosten für Plattform und Groupware beheben lassen. Die Wartung und Pflege der Benutzeraccounts wird durch eine Anbindung an ActiveDirectory zentral erledigt.

#### 4.2.4.5.2 Zarafa

Zarafa ist eine Groupware-Lösung, die die Exchange-Funktionalität von Grund auf neu implementiert hat und auf dem Markt zunehmend Verbreitung findet. Zarafa erinnert nicht nur optisch auf den ersten Blick stark an Exchange. Die für Linux entwickelte Groupware wurde an Exchange angelehnt und bildet dessen Funktionen nach. Dabei ist Zarafa Mitglied der Lisog[32] und unterstützt die OpenMAPI Initiative, die im Jahre 2008 von verschiedenen Firmen im Groupware-Bereich gegründet wurde, um alternative Schnittstellen auf Basis des proprietären MAPI zu schaffen. Das niederländische Unternehmen Zarafa veröffentlichte Ende Juni 2011 mit der Zarafa Collaboation Platform 7.0 die aktuelleste Version seiner Groupware.

Zarafa ist ein Open-Core Produkt, das kommerziell vertrieben wird, aber eine eingeschränkte Open-Source Edition mit reduziertem Funktionsumfang und Verbindungsmöglichkeiten für Clients anbietet. Zarafa wird in einer reinen OSS-Variante und mit drei verschiedenen Open-Core-Lizenzen angeboten. Die freie Community Edition lässt zwar einen unbegrenzten Zugriff per Webinterface und IMAP zu, unterstützt aber maximal eine Verbindung von drei Outlook-Clients. Außerdem fehlen ihr nützliche Features wie der Mehrbenutzer-Kalender, eine integrierte Backup-Funktion oder die AD-Unterstützung. Diese Funktionen sind in der Standard Edition (Small Business) enthalten. Die Professional Variante erweitert diese durch einen Blackberry-Enterprise-Server, eine automatische Software-Verteilung (Auto Deployment Tools) und Hochverfügbarkeitsfunktionen. Die Lizenz mit dem größten Umfang ist die Enterprise Edition, mit der Multi-Server-Architekturen ermöglicht werden. Zarafa selbst gibt an, dass bei gleicher Funktionalität im Vergleich zum Einsatz eines Exchange Servers nur die halben Kosten anfallen.

Die Grundfunktionalität mit E-Mail, Kalender, Kontakten und einer Aufgabenliste wird von Zarafa abgedeckt. Zusätzlich können Verzeichnisse auf dem Zarafa-Server angelegt werden, in denen Benutzer Daten ablegen können. Der Zugriff ist für jeden Benutzer und Ordner einzeln konfigurierbar. Ein eigener, moderner, AJAX-basierter WebClient ist in der Groupware integriert, so dass auch per Browser ohne eigenen PIM die angebotenen Funktionen genutzt werden können.

Als einzige Systemvoraussetzung bedingt Zarafa Linux als Server-Plattform. Binaries für die verbreitetsten Linux-Distributionen werden bereitgestellt, so dass keine Sourcen kompiliert werden müssen. Zarafa baut auf bereits vorhandene Komponenten auf, verwendet zur Datenhaltung die Datenbank MySQL und benötigt einen Mail Transport Agent (MTA), einen Webserver und einen Virus- und Spamfilter. Hierfür nutzt Zarafa OSS-Lösungen wie Postfix, Exim, qmail oder Sendmail als MTA. Apache mit PHP wird als Webserver unterstützt, SpamAssassin und ClamAV sorgen für den Schutz vor unerwünschten E-Mails. Außerdem wird die Sicherheit durch die optionale Verwendung der gängigen Verschlüsselungsmethoden von Verbindungen (TLS/SSL) und E-Mails gewährleistet.

An Protokollen und Formaten verwendet Zarafa gängige offene Standards wie POP3 und IMAP für E-Mail, iCal und CalDAV für den Kalender sowie zusätzlich noch OpenMAPI. Für die Synchronisation mit mobilen Geräten sorgt Z-Push, eine Eigenentwicklung von Zarafa und Implementierung von ActiveSync OVA (Over-The-Air). Durch dieses Spektrum an möglichen Verbindungsvarianten können nach Herstellerangaben Smart Phones mit Windows Mobile, iOS oder Android sowie alle Arten von Clients oder PIM Daten mit Zarafa austauschen.

Eine Besonderheit gibt es bei Zarafa bei der Erweiterbarkeit. Zarafa bietet mit Z-Merge ein Framework an, über das andere Software die Komponenten von Zarafa mit nutzen kann. So gibt es zum Beispiel Plug-Ins für SugarCRM, Alfresco und Google Maps. Eine vollständige Liste der integrierbaren Applikationen findet sich auf der Homepage von Zarafa[33].

Im Gegensatz zu Exchange wird bei Zarafa kein allumfassendes Produkt geliefert, das ohne jede weitere Software auskommt. Um die Groupware einsetzen zu können, wird ein LAMP-Server (LDAP, Apache, MySQL und PHP) als Infrastruktur benötigt. Diese Komponenten sind allerdings frei verfügbar, in jeder Linux-Distribution problemlos installierbar und weisen einen sehr geringen Ressourcenbedarf auf.

[32] Linux Solutions Group e.V.

[33] http://zarafa.com/integrations

#### 4.2.4.5.3 Kolab

Kolab ist die Groupware-Lösung der Kolab Systems AG, ehemals Kolab Konsortium, und als reine Open-Source-Software in vollem Umfang frei verfügbar. Der Hersteller veröffentlichte die aktuelle Version 2.3.2 im Juni 2011. Kolab baut dabei auf den Konzepten auf, die in der Kolab Format Specifikation[34] und dem Kolab Architecture Paper[35] festgehalten sind. Ursprünglich wurde Kolab zwischen 2002 und 2004 für das BSI entwickelt und dort auch zum ersten mal eingesetzt. Im November 2005 gewann Kolab den Linux New Media Award in der Kategorie "Bester Groupware Server"[36].

Kolab nutzt IMAP als zentrales Protokoll nicht nur zum Abrufen von E-Mails. Auch für das Adressbuch und den Kalender werden die Einträge in besonderen Verzeichnissen gespeichert, deren Zugriffsrechte und Abruf ebenfalls über IMAP und ACLs abgewickelt werden. Die von Kolab verwendeten Standards – neben IMAP sind dies vor allem POP3 und SyncML – sind offen und etabliert. Die Konfiguration und Verwaltung des Kolab Server erfolgt dabei weitestgehend unter Verwendung von LDAP. Entwickelt wurde Kolab mit dem Personal Information Manager Kontact als Referenz-Client. Dabei sind mit E-Mail, Adressbuch, Kalender und Aufgabenliste die wichtigsten Grundfunktionalitäten implementiert. ActiveSync-fähige Geräte können zudem über Z-Push mit dem Kolab Server synchronisiert werden.

Kolab bietet ein globales Adressbuch, Gruppenkontakte und persönliche Kontakte. Mittels ACLs können hier feingranulare Freigaben zwischen verschiedenen Benutzer verwirklicht werden. Als E-Mail-Server bringt Kolab keine eigenen Dienste mit, sondern verwendet offene, bereits gut erprobte Standard-Infrastrukturkomponenten wie Postfix, OpenLDAP und Cyrus. Dies führt zu einer sehr großen und guten Skalierbarkeit und einem geringen Ressourcenverbrauch, wodurch ein Kolab Server nicht dediziert betrieben werden muss. Als Systemvoraussetzung bedingt Kolab einen Linux- oder Unix-Server.

Kolab bietet eine Web-Schnittstelle zur Administration der Groupware. Dabei werden drei Privilegienstufen verwendet, mit denen die Wartung des Servers ohne Administrator-Rechte ermöglicht wird. Kolab kann durch die Installation von zusätzlicher Software wie Horde um ein Web-Interface erweitert werden, über das Benutzer die Groupware auch per Browser nutzen können. An den Komfort seiner Konkurrenten kommt diese Lösung allerdings nicht heran.

Kolab sieht neben der OSS-Lizenz keine weiteren Varianten vor, alle Komponenten sind frei nutzbar. Die offenen Standards sorgen für Investitionssicherheit (siehe 2.5.5) und gleichzeitig dafür, dass jeder PIM zum vollwertigen Kolab-Client erweitert werden kann.

Zur Anbindung von Outlook-Clients können proprietäre Plug-Ins von Dritten bezogen werden. Thunderbird kann nach der Installation des Plug-Ins SyncKolab zum Kolab-Client erweitert werden, für Evolution gibt es wie auch für die Verbindung zu Exchange das Paket evolution-kolab. Eine Übersicht verschiedener Clients und Plug-Ins sowie eine Anleitung zum Einrichten derselben stellt Kolab in seinem Wiki[37] zur Verfügung. Dort findet sich auch eine Übersicht über die Kompatibilität der Groupware mit unterschiedlichen Clients. Kontact als Referenz-Client steht alternativ und ohne Anpassungsbedarf ebenfalls als OSS zur Verfügung.

Hinsichtlich der IT-Sicherheit entspricht Kolab den üblichen Standards. Die Verbindung zum Server kann über TSL/SSL abgesichert, E-Mails können mit OpenPGP oder S/MIME verschlüsselt und/oder signiert werden. Als Viren- und Spamfilter werden in der Regel die mitgelieferten Spamassasin und ClamAV verwendet; es besteht aber die Möglichkeit, andere Lösungen zu integrieren. Eine Besonderheit unter den Groupware-Lösungen ist das Konzept „Everything is a File“. Alle Daten werden in Form von Dateien direkt auf dem Server im Dateisystem gespeichert, es wird keine Datenbank verwendet. Dadurch kann ein Backup aller Daten auf dem Server automatisiert und mit den Bordmitteln des Betriebssystems durchgeführt werden. Zur Erhöhung der Kapazität und Verfügbarkeit können Kolab-Server auch als Slave-Server an mehreren Standorten mit einer anderen Instanz verbunden oder mittels OpenLDAP-Proxy und verteilten Mailboxen als Cluster betrieben werden.

[34] http://www.kolab.org/doc/kolabformat-2.0.pdf
[35] http://www.kolab.org/doc/concept-draft-cvs20060921.pdf
[36] http://www.kolab.org/news/pr-20051115.html
[37] http://wiki.kolab.org/Main_Page

#### 4.2.4.6 Bewertungstabelle

Tabelle 4.5: Vergleich Groupware

| Groupware | Exchange | Zarafa | Kolab |
|---|---|---|---|
| **Funktionen** | | | |
| E-Mail | ✓ | ✓[38] | ✓[38] |
| Kalender | ✓ | ✓ | ✓ |
| Adressbuch | ✓ | ✓ | ✓ |
| Aufgabenliste | ✓ | ✓ | ✓ |
| Notizen | ✓ | – | – |
| Dokumentenverwaltung | ✓ | ✓ | – |
| Web-Frontend | ✓ | ✓ | ✓[39] |
| **Lizenzierung** | | | |
| | Proprietär | OpenCore | OpenSource |
| **Protokolle und Synchronisation** | | | |
| IMAP/POP3 | ✓[40] | ✓ | ✓ |
| MAPI | ✓ | ✓[41] | – |
| ActiceSync | ✓ | ✓ | ✓ |
| SyncML | ✓ | ✓ | – |
| LDAP | ✓ | ✓ | ✓ |
| **Sicherheit** | | | |
| TLS/SSL | ✓ | ✓ | ✓ |
| Spamfilter | ✓ | ✓ | ✓ |
| Blacklisting | ✓ | – | – |
| Virenscanner | ✓ | ✓ | ✓ |
| Backup | ✓ | ✓ | ✓[42] |
| OpenPGP / S/MIME | ✓ | ✓ | ✓ |
| Clusterfähigkeit | ✓[43] | ✓[43] | – |

#### 4.2.4.7 Empfehlungen

Die umfangreichste Funktionalität bietet der Microsoft Exchange Server, sofern er im Zusammenspiel mit Microsoft Outlook oder anderen MAPI-fähigen Clients eingesetzt wird. In heterogenen Umgebungen und beim Einsatz alternativer PIM ohne MAPI-Unterstützung reduziert sich dieser Vorsprung stark. Von den untersuchten Exchange-Alternativen bietet Zarafa die meisten Möglichkeiten zur Synchronisation

[38] baut auf anderen Komponenten auf
[39] nur über zusätzliche Software
[40] IMAP muss explizit freigeschalten werden
[41] implementiert durch OpenMAPI
[42] keine Funktion vorhanden, kann aber manuell auf Dateiebene eingerichtet werden
[43] je nach Version

und Kommunikation mit Clients und ist dadurch unabhängig von Clients und deren Betriebssystemen in vollem Umfang nutzbar. Verbindungen zu Outlook über MAPI sind mit Zarafa genauso möglich wie zu Linux-Clients oder allen gängigen Smartphones. Die wesentlichen Protokolle und Methoden sind ohne Zusatzinstallationen auf Server- oder Client-Seite enthalten, während bei Kolab die volle Konnektivität erst durch Plug-Ins im Client hergestellt werden muss.

Kostenseitig ist Kolab durch die OSS-Lizenzierung und den ausschließlichen Einsatz offener Standards prinzipiell im Vorteil[44]; Zarafa verursacht im professionellen Einsatz (Professional oder Enterprise Edition) im Vergleich zu Exchange moderate Kosten und bietet einen Rabatt für öffentliche Einrichtungen von 25%. Hinsichtlich der Hardware-Anforderungen und Systemvoraussetzungen sind Kolab und Zarafa vergleichbar genügsam. Microsoft Exchange Server benötigt neben der hauseigenen Plattform Windows Server weitere Lizenzkosten-trächtige Komponenten, insbesondere den Verzeichnisdienst AD, und stellt die vergleichsweise höchsten Anforderungen an die Server-Hardware. Insbesondere bei vielen angebundenen Clients und dadurch zusätzlich benötigten Server-Instanzen müssen hohe Kosten veranschlagt werden.

Insgesamt bietet der Exchange Server nur in homogenen Microsoft-Umgebungen wesentliche Vorteile und verursacht vergleichsweise hohe Kosten. Zarafa hingegen bietet basierend auf erprobten Technologien den Komfort von Exchange, kann mittels des Z-Merge Replication Frameworks in viele Anwendungen integriert werden und skaliert ressourcenschonend auch für eine große und wachsende Anzahl an Benutzern. Kolab ist ein verlässliches Werkzeug mit erprobten Komponenten und geringen unmittelbaren Kosten, bietet aber nur wenig Bedienkomfort und lückenhafte Konnektivität.

Bei einer Migration gilt es zu beachten, dass der Weg von und zu Microsoft Exchange mit seinen proprietäten Formaten nicht ohne größeren Aufwand möglich ist. Alternative Lösungen mit einer der gängigen Open-Source-Infrastrukturen wie LAMP (s.o.) und der Einhaltung der wesentlichen offenen Standards können hingegen meist einfach gegeneinander ausgetauscht werden. Bei der Migration von oder zu Exchange Server muss zusätzlicher Aufwand für Datenkonvertierungen eingeplant werden. Die Hinzuziehung externer Experten ist ratsam.

#### 4.2.4.8 Migrations-Checkliste

Die nachfolgende Checkliste stellt sicher, dass bei der Migration im Bereich Groupware-Server alle relevanten Aspekte berücksichtigt werden. Die unter den Arbeitsschritten stehenden Informationen zeigen, wie die Bewertungskriterien konkretisiert werden können.

##### 4.2.4.8.1 Projektbüro einrichten

1. Planung der Migration
2. Einteilung der Behörde in Migrations-Gruppen
3. Erstellung von Prüflisten für die Ist-Analyse

##### 4.2.4.8.2 Ist-Analyse gruppenweise durchführen

1. Bisher eingesetzte Serverstruktur und Groupware ermitteln
2. Informationen über verwendete PIM beschaffen
3. Verteilung der Betriebssysteme auf den Arbeitsplatzrechnern
4. Derzeit unterstützte und verwendete Funktionen
5. Domänenspezifische Bewertungskriterien

[44] Siehe Abschnitt 2.6.3

#### 4.2.4.8.3 Ist-Analyse auswerten

1. Liste mit Mindest-Anforderungen an die Basisfunktionalität
2. Liste mit spezifischen Zusatz-Anforderungen
3. Priorisierung der Anforderungen
4. Konsolidieren der gewonnenen Erkenntnisse

#### 4.2.4.8.4 Bewertung und Entscheidung

1. Festlegen der maßgeblichen Standards und Protokolle
2. Vorauswahl der Prüfkandidaten
3. Zuordnung der einzelnen Anforderungen zur Groupware und sonstigen Komponenten wie Verzeichnisdiensten
4. Domänenspezifika festlegen
5. Abgleich der Mindest-Anforderungen an die Basisfunktionalität mit Funktionalitäten der Produkte
6. Notwendigkeit zur Festlegung eines PIM
7. Möglichkeiten für Migration evaluieren und planen

### 4.2.5 Virtualisierung und Terminaldienste

Die Themen Virtualisierung und Terminaldienste sind Facetten des zunehmenden Trends, den IT-Betrieb zu konsolidieren und von konkreter Hardware zu abstrahieren. Neben Vorteilen bei der Verwaltung des vorhandenen Rechnerparks helfen beide Themen auch bei der Beschaffung neuer Hardware, da standardisierte Plattformen für beliebige Einsatzzwecke geschaffen und ggf. Client-seitig die Anforderungen reduziert und damit günstigere Geräte beschafft oder zur Aussonderung vorgesehene weiter verwendet werden können.

Seit der letzten Veröffentlichung des Migrationsleitfadens hat das Thema Virtualisierung stark an Bedeutung gewonnen. Insbesondere für das sogenannte Cloud Computing ist die Abstraktion von der physikalischen Umgebung eine häufig genutzte Möglichkeit, um viele Server-Systeme parallel betreiben und die vorhandene oder zu beschaffende Hardware dabei optimal auslasten zu können. Die Virtualisierung unterstützt daher die Anforderungen an eine Green IT[45], bietet aber auch auf der Desktop-Seite Vorteile und nimmt unter den Stichworten Virtual Desktop Infrastructure (VDI) und Anwendungsvirtualisierung inzwischen breiten Raum ein.

Dieses Unterkapitel widmet sich zunächst der Erläuterung zentraler Begriffe der Virtualisierung, um anschließend die Server-, die Desktop- und die Anwendungs-Virtualisierung in Bezug auf Software-Migrationen zu beleuchten, und endet mit einem Überblick über Terminal-Lösungen.

#### 4.2.5.1 Einleitung

Die von IBM bekannte logische Systemaufteilung von Großsystemen (Logical Partitioning, LPAR) ist zwar ein Nischenprodukt geblieben, deren Prinzipien sind allerdings dieselben, die auch heutige Virtualisierungslösungen prägen. Diese bestehen aus einem Wirts- und einem oder mehreren Gastsystemen. Das Wirtssystem greift unmittelbar auf die physikalische Hardware zu und bietet über eine Abstraktionsschicht ein emuliertes Umfeld an Komponenten, auf denen Gastsysteme wie auf einem physikalischen Rechner installiert werden können. Diese Abstraktionsschicht wird üblicherweise Hypervisor oder Virtual Machine Monitor genannt. Sie ist für die Weiterleitung der Zugriffe aus der virtuellen Maschine (VM) auf die tatsächliche Hardware verantwortlich. Da diese Weiterleitung die Verarbeitungsgeschwindigkeit deutlich senken kann, verfolgen Hard- und Softwarehersteller verschiedene Ansätze zu deren Beschleunigung, beispielsweise die Paravirtualisierung.

##### 4.2.5.1.1 Voll- und Paravirtualisierung

Virtualisierungslösungen unterscheiden sich darin, ob der jeweilige Hypervisor ein System vollständig (Vollvirtualisierung) oder nur teilweise emuliert (Paravirtualisierung). Bei der Vollvirtualisierung stellt der Hypervisor den Gastsystemen eine vollständig emulierte Hardwareumgebung zur Verfügung und übernimmt sämtliche Systemaufrufe über die Emulationsschicht. Gastsysteme können unverändert auf dieser Emulationsschicht installiert und betrieben werden, deren Verarbeitungsgeschwindigkeit ist allerdings im Vergleich zum nicht emulierten Betrieb deutlich geringer.

Bei der Paravirtualisierung emuliert der Hypervisor nur einen geringen Teil der Hardware und nutzt für die übrigen Teile fremde Resourcen. Dies kann entweder entsprechende Hardwareunterstützung oder ein sogenanntes privilegiertes Gastsystem sein, welches entsprechende Zugriffsmöglichkeiten bietet und selbst wiederum auf den vom Hypervisor bereitgestellten emulierten Teil der Systemaufrufe zugreifen muss. Das privilegierte Gastsystem ist folglich an mehreren Stellen an die paravirtuelle Systemumgebung anzupassen; unveränderbare Betriebssysteme wie Microsoft Windows scheiden daher als privilegierte Gastsysteme aus. Die Verarbeitungsgeschwindigkeit der nicht emulierten Systemzugriffe des privilegierten Gastsystems entspricht der einer Standard-Installation ohne Hypervisor, es ist damit das schnellste mögliche Gastsystem.

[45] http://www.cio.bund.de/green-it

Unprivliegierte Gastsysteme haben keinen unmittelbaren Systemzugriff. Sie müssen daher entweder so angepasst werden, dass sie sowohl die emulierten Systemaufrufe als auch die o.g. spezifischen Schnittstellen des Hypervisors über entsprechende Bibliotheken nutzen (**explizite Paravirtualisierung**). Oder das Wirtssystem verfügt über Prozessoren mit Erweiterungen wie AMD-V oder Intel VT, die den wesentlichen Funktionsumfang solcher Bibliotheken auf der Hardware-Ebene abbilden. Diese Konstellation wird als *Hardware Virtual Machine (HVM)* bezeichnet und ermöglicht eine für Gastsysteme **transparente Paravirtualisierung** ohne jede Änderung. Aktuelle Hypervisor können vorhandene hardwareseitige Virtualisierungsfunktionen nutzen und bieten dann die transparente Paravirtualisierung an. Das steigert die Verarbeitungsgeschwindigkeit unveränderter Gastsysteme deutlich und führt in Kombination mit optimierten Gerätetreibern[46] zu Performance-Werten, die sich nur noch wenig von denen nicht virtualisierter Systeme unterscheiden.

#### 4.2.5.1.2 Hypervisor-Typen

Neben der Voll- und der Paravirtualisierung werden Hypervisor auch dahingehend unterschieden, ob sie auf einer physikalischen Maschine unmittelbar als unterste Schicht installiert werden (**Hypervisor Typ 1**, „bare metal“), oder ob sie ein installiertes Betriebssystem um Virtualisierungsfunktionen erweitern (**Hypervisor Typ 2**). Während Hypervisor vom Typ 2 bereits auf eine vollständige Hardware-Unterstützung des Wirtssystems zurückgreifen können, müssen „bare metal“-Hypervisor eigene Treiber mitbringen. Zur Vermeidung entsprechender Aufwände werden Typ 1-Hypervisor daher entweder mit Varianten aktueller Betriebssysteme kombiniert, die auf Funktionen zur Virtualisierungsunterstützung reduziert sind, oder sie nutzen privilegierte Gastsysteme und deren Treiber.

#### 4.2.5.1.3 Virtualisierungsarten

Je nach Einsatzzweck und -ort werden verschiedene Arten von Virtualisierung unterschieden. Gängig ist derzeit die Unterscheidung nach Server-, Desktop- und Anwendungs-Virtualisierung.

**Server-Virtualisierung** bezeichnet den Betrieb eines oder mehrerer im Gesamtsystem bereitgestellter Dienste und der für deren Funktionieren notwendigen Betriebs- und Teilsysteme in einer virtuellen Maschine auf einem Server. Ein Dienst und die dafür notwendigen Teilsysteme können auch in je eigenen virtuellen Maschinen betrieben werden.

**Desktop-Virtualisierung** oder *Virtual Desktop Infrastructure* bezeichnet die Bereitstellung eines Standard-Arbeitsplatzrechners (Desktops) als virtuelle Maschine für verschiedene Anwender auf einem Server. Deren spezifische Daten werden getrennt vom Standard-Desktop vorgehalten, die Zuordnung eines Standard-Desktops und der spezifischen Daten zu einem Anwender wird von einer Vermittlungsinstanz hergestellt. Der Anwender nutzt hauptsächlich den virtuellen anstelle des lokalen Desktops.

**Anwendungs-Virtualisierung** bezeichnet die möglichst transparente Bereitstellung einer einzelnen Anwendung oder einer Anwendungsgruppe samt dem notwendigen Unterbau (Betriebssystem, Hilfsprogramme) in virtualisierter Form auf dem lokalen Arbeitsplatzrechner eines Anwenders.

#### 4.2.5.1.4 Speicherformate

Virtuelle Maschinen werden von den verschiedenen Lösungen in unterschiedlichen Formaten abgelegt. Allen gemeinsam sind eine virtuelle Festplatte, auf der das Gastsystem gespeichert wird, und Konfigurationsparameter, die Art und Umfang der virtuellen Komponenten bestimmen, beispielsweise die Anzahl an Prozessoren oder die Größe des Hauptspeichers.

Die virtuelle Festplatte ist eine Datei, die in verschiedenen Formaten vorliegen kann. Verbreitet sind die Formate Virtual Machine Disk (VMDK), Virtual Desktop Image (VDI), Virtual Hard Disk (VHD) und QE-

[46] VirtIO bietet beispielsweise für die Virtualisierung optimierte Treiber für den Zugriff auf Netzwerkkarten und Festplatten.)

MU Copy On Write (QCOW). Die bei älteren Dateisystemen noch notwendige Aufteilung der virtuellen Festplatte in 2-GByte-Stücke ist inzwischen überholt. Bei der Erstellung einer virtuellen Festplatte muss deren maximale Kapazität zwar definiert, aber nicht sofort alloziiert werden. Vielmehr kann die tatsächliche Größe einer virtuellen Festplatte mit dem Bedarf des Gastsystems mitwachsen. Dies ermöglicht die Definition hoher virtueller Kapazitäten als Plattform für verschiedene Zwecke, die auch Spitzenbelastungen standhält, ohne dabei den physikalischen Speicherbedarf und die damit verbundenen Kosten über zu strapazieren.

#### 4.2.5.1.5 Zugriff

Auf virtuelle Systeme wird entweder lokal (Anwendungs-Virtualisierung) oder über Netzwerk-Protokolle zugegriffen (Desktop- und Server-Virtualisierung). Bei der Server-Virtualisierung kann auf die virtualisierten Dienste über die für den jeweiligen Dienst üblichen Protokolle zugegriffen werden – es besteht für die Dienstnutzung kein Unterschied zwischen einer Dienst-Installation auf einer physikalischen oder einer virtuellen Maschine. Für den Zugriff auf den Hypervisor zur Verwaltung der virtuellen Maschinen werden hingegen spezifische Protokolle je Virtualisierungslösung genutzt. Dies gilt gleichermaßen für den Hypervisor-Zugriff bei der Desktop-Virtualisierung. Hier muss zusätzlich der virtualisierte Desktop mit den Ein- und Ausgabe-Komponenten des lokalen Arbeitsplatzrechners wie Tastatur, Maus und Bildschirmausgabe verbunden werden. Dafür existieren diverse Protokolle, gebräuchlich sind Remote Desktop Protocol (RDP), Citrix ICA, Simple Protocol for Independent Computing Environments (SPICE) und das von Virtual Network Computing (VNC) bekannte Remote Framebuffer Protocol (RFB).

#### 4.2.5.1.6 Offene Standards

Für den Fernzugriff auf grafische Benutzerschnittstellen existiert mit dem o.g. RFB ein offener und Plattform-unabhängiger Standard, der allerdings durch die Übertragung von Grafik als einzelne Pixel deutlich mehr Bandbreite benötigt als Protokolle wie das X Window System oder RDP, die Grafik-Primitive austauschen. Durch die weite Verbreitung von VNC und verschiedene Optimierungen in der Datenübertragung ist RFB allerdings neben RDP weiterhin das häufigste derartige Zugriffsprotokoll.

Das von Microsoft entwickelte RDP basiert auf der offen standardisierten ITU T.120 Protokollfamilie. Die spezifischen Erweiterungen sind aber weder offen standardisiert noch vom Microsoft'schen „Open Specification Promise“ umfasst, sondern vielmehr Lizenz-bewehrt und durch Patente geschützt. Trotzdem existieren freie Implementierungen von RDP-Servern und -Clients[47], die allerdings nur Teile des gesamten RDP-Umfangs abdecken und regelmäßig auf früheren Versionen des Protokolls beruhen. RDP gilt heute als nur mäßig effektiv im Umgang mit Systemresourcen, zudem sind viele Erweiterungen in den jüngsten Protokoll-Versionen auf die Verwendung durch Microsoft-Betriebssysteme eingeschränkt.

Mit SPICE existiert ein noch junges offenes Protokoll für die sogenannte Virtual Desktop Infrastructure, welches die optimale Nutzung der beteiligten Komponenten hinsichtlich Netzwerkbandbreite und Rendering-Kapazitäten[48] zum Ziel hat. Die von Red Hat als *Emerging Technology* vorangetriebene OSS-Implementierung des Protokolls weist bereits einen praxistauglichen Umfang auf[49], hat aber abgesehen von der *Red Hat Enterprise Virtualization for Desktops* noch keine Verbreitung gefunden.

Mit dem System Virtualization Model[50] hat die DMTF u.a. unter Beteiligung des Marktführers VMware ein offenes Modell zur Verwaltung virtualisierter Systeme auf der Basis des hauseigenen Common Information Model (CIM) erstellt, welches beispielsweise vom OSS-Projekt libvirt implementiert ist. Das Open Virtualization Format (OVF) ist ein ebenfalls von der DMTF entwickelter offener Standard für das Verpacken und Bereitstellen virtueller Maschinen zusammen mit Meta-Informationen wie der Anzahl an CPUs. Das Ziel des Standards ist eine Vereinheitlichung wesentlicher Informationen über virtuelle Maschinen zum Austausch zwischen verschiedenen Virtualisierungslösungen. Verpackt werden können

[47] Beispielsweise http://www.xrdp.org und http://www.freerdp.com
[48] Unter Rendering wird die Übersetzung grafischer Beschreibungen in physikalische Pixel verstanden.
[49] Siehe http://www.spicespace.org/features.html
[50] Siehe http://www.dmtf.org/sites/default/files/standards/documents/DSP2013_1.0.0.pdf

eine oder mehrere virtuelle Maschinen gemeinsam. Damit ist die gleichzeitige Bereitstellung aufeinander abgestimmter virtueller Maschinen möglich, was auch als *vApps* bezeichnet wird.

Die von VMware 2006 veröffentlichte Spezifikation eines *Virtual Machine Interface (VMI)*[51] beschreibt eine Schnittstelle für die Paravirtualisierung. Teile davon flossen unter dem Namen „paravirt-ops“ für eine transparente Paravirtualisierung von Linux-Systemen unter dem XEN-Hypervisor in den Linux-Kernel ein, sind aber aufgrund der inzwischen verbreiteten Hardware-Unterstützung obsolet geworden.

Wesentliche Aspekte von Virtualisierungslösungen wie der Zugriff auf den Hypervisor oder das Format virtueller Festplatten sind allerdings bis heute nicht standardisiert. Die diese Punkte thematisierende „Open Hypervisor Standards“-Initiative vom Marktführer VMware aus dem Jahr 2005[52] blieb erfolglos. Mögliche Standardisierungsansätze der DMTF sind nur für Mitglieder einsehbar, das Institute of Electrical and Electronics Engineers (IEEE) listet keine eigenen Initiativen.

Immerhin sind die gängigsten Formate virtueller Festplatten frei einsehbar, entweder in Form von Spezifikationen[53] oder von Implementierungen[54], und können von alternativen Implementierungen frei genutzt werden. Und mit der Open Virtualization Alliance (OVA)[55] wurde 2011 eine Organisation gegründet, deren erklärte Ziele die Nutzung von offenen Virtualisierungstechnologien wie der Kernel-based Virtual Machine (KVM), die Unabhängigkeit von proprietären Virtualisierungslösungen und die Förderung von Interoperabilität zwischen verschiedenen solchen Produkten sind. Über das Cloud Computing (siehe Unterkapitel 5.1) kommt zudem weiterer Schwung in die Thematik.

#### 4.2.5.2 Kriterien

Die Virtualisierung von Systemen bietet eine günstige Möglichkeit, vorhandene Abhängigkeiten zu identifizieren, zu modularisieren oder aufzulösen. Um hierbei nicht in weitere Abhängigkeiten zu geraten, sollten mögliche Virtualisierungslösungen dahingehend geprüft werden, unter welchen **Lizenzen** sie verfügbar sind und welche generellen **Einschränkungen** bestehen. Hinsichtlich deren Grundfunktionalität sollte geprüft werden, welche **Wirts- und Gastsysteme** möglich sind, ob sie für den Betrieb **angepasst** werden müssen, ob vorhandene **Hardware-Unterstützung** wie Intel VT-x und AMD-V zur Performance-Steigerung genutzt wird und welche **VM-Formate** unterstützt werden.

**Verwaltungswerkzeuge** für virtuelle Maschinen sollten diese zur Laufzeit auf einen anderen physikalischen Rechner **verlagern** (Live-Migration) und **Zwischenstände** (Snapshots) erstellen können. Beim **Kopieren** von als Vorlage dienenden virtuellen Maschinen (Klonen) sollten deren Identifikationsmerkmale automatisiert angepasst werden, um mehrere Klone parallel betreiben zu können. **OVF**-Pakete sollten erzeugt und importiert und verschiedene Hypervisor über eine einheitliche Oberfläche administriert werden können.

Für die Desktop-Virtualisierung sollte zusätzlich betrachtet werden, über welche **Protokolle** auf ein entferntes Gastsystem zugegriffen und ob es auch lokal genutzt werden kann (**Offline-Fähigkeit**), ob lokale, insbesondere **USB-Geräte**, an das Gastsystem weitergereicht werden können und ob zumindest grundsätzliche **multimediale Fähigkeiten** wie Videostreaming, Audioweiterleitung und die Verwendung mehrerer Monitore unterstützt werden. Angesichts vieler paralleler Instanzen von Standard-Desktops sollte die Virtualisierungslösung den **physikalischen Resourcenbedarf** auf dem Wirtssystem durch geeignete Maßnahmen deutlich unter den nominellen Werten der Gastsysteme halten und **Benutzerspezifika** von den Standard-Desktops getrennt verwalten.

Lösungen für die Anwendungs-Virtualisierung sollten sich gut in den lokalen Desktop **integrieren** und die Nutzung einer virtuellen Anwendung für den Anwender möglichst transparent gestalten. **Drag&Drop** zwischen lokaler und virtueller Anwendung sollte ebenso unterstützt werden wie das gemeinsame Verwenden des **Clipboards** und derselben **Speicherorte**. Ein expliziter **Eingabefokuswechsel** zwischen

[51] Siehe http://www.vmware.com/pdf/vmi_specs.pdf
[52] Siehe http://www.vmware.com/company/news/releases/community_source.html
[53] Siehe VMDK, VHD und QCOW
[54] Dies gilt insbesondere für das von Oracle VirtualBox verwendete Format VDI.
[55] http://www.openvirtualizationalliance.org, Mitglieder sind u.a. HP, IBM, Intel und Red Hat.

lokalen und virtuellen Anwendungen sollte nicht notwendig und dafür ggf. vorgesehene sogenannte **Gasterweiterungen** für alle untersuchten Plattformen verfügbar sein. Die Virtualisierungslösung sollte **Hilfsmittel zur einfachen Erstellung** virtueller Maschinen für das jeweilige Gast-Betriebssystem bieten und die VM in einem gebräuchlichen **Format** speichern.

#### 4.2.5.3 Ist-Analyse

Zunächst gilt es, die derzeit eingesetzten Virtualisierungslösungen und die damit virtualisierten Systeme zu erfassen. Dabei sollte ermittelt werden,

- in welchen Bereichen (Infrastruktur, Desktop, Querschnitts- oder Fachanwendungen, jeweils unterteilt in Entwicklung, Test, Produktion) virtuelle Systeme genutzt werden,
- welche Virtualisierungslösungen in welcher Version eingesetzt werden,
- mit welchen Werkzeugen die virtuellen Systeme verwaltet werden,
- welcher Aufwand mit der Einrichtung und Verwaltung virtueller und Wirtssysteme verbunden ist,
- ob die virtuellen Systeme zentral oder verteilt verwaltet werden,
- welche und wie viele Lizenzen für die Virtualisierungslösungen, die Wirtssysteme und die virtualisierten Systeme benötigt werden,
- in welchen Formaten die virtuellen Systeme vorliegen,
- welche virtuellen Systeme mit welchen Gasterweiterungen versehen sind,
- auf welchen Wirtssystemen die virtuellen Systeme betrieben werden,
- welcher Art von Virtualisierung (Server-, Desktop-, Anwendungs-Virtualisierung) das jeweilige virtuelle System entspricht,
- wie hoch die durchschnittliche und die Spitzenbelastung der Resourcen der Wirtssysteme liegen und
- ob virtuelle Maschinen in Form von Vorlagen existieren und in welchem Ausmaß diese verwendet werden.

Diese Informationen sollten dahingehend konsolidiert werden, dass daraus die Verteilung der Virtualisierungslösungen hervorgeht und Rückschlüsse auf die Erfahrung im Umgang mit virtualisierten Systemen sowohl bei der IT-Administration als auch bei Benutzern von Desktop- und Anwendungs-Virtualisierungen möglich sind. Die vorhandenen Virtualisierungslösungen sollten hinsichtlich ihrer Abhängigkeit von bestimmten Wirtssystemen, ihrer Komplexität und Bedienbarkeit bewertet werden. Zudem sollten die verwendeten und alternative Verwaltungswerkzeuge ermittelt und verglichen und möglichst eine Tendenz für den physikalischen Resourcenbedarf hergeleitet werden.

#### 4.2.5.4 Soll-Konzeption

Der erste Schritt der Soll-Konzeption ist die Ermittlung des künftigen Bedarfs an virtualisierten Systemen. Die Virtualisierung ist kein Selbstzweck, sondern sollte stets im Zusammenhang mit anderen Zielen des IT-Umfelds eingesetzt werden.

Eine Anwendungs-Virtualisierung sollte in Betracht gezogen werden, wenn Querschnitts- oder Fachanwendungen zwar lokal ausgeführt werden müssen, aber den lokalen Arbeitsplatz nicht verändern sollen oder in mehreren Versionen benötigt werden. Sie ermöglicht zudem das zentralisierte Einspielen von Sicherheitsupdates und verhindert die Kompromittierung lokaler Arbeitsplatzrechner über Sicherheitslücken in diesen Anwendungen.

Die Desktop-Virtualisierung kann ebenfalls durch zentral verwaltete und aktualisierte Standardsysteme zu einem verringerten Administrationsaufwand je Arbeitsplatzrechner führen und zugleich das Sicherheitsniveau durch zentral eingespielte Updates verbessern. Die Datensicherung kann auf die Standard-

systemvorlagen und die tatsächlichen Anwenderdaten reduziert und automatisiert werden. Vorhandene Arbeitsplatzrechner können durch die Verlagerung grafik- oder rechenintensiver Anwendungen auf leistungsfähige Systeme länger genutzt und ggf. durch Thin Clients ohne eigene Speicherkapazitäten ersetzt werden.

Eine (verstärkte) Server-Virtualisierung kann beispielsweise sinnvoll sein, wenn die Belastung vorhandener Server-Hardware besser verteilt, die Hochverfügbarkeit von Diensten gewährleistet oder die Energieeffizienz von Serversystemen verbessert werden soll. Auch kann sie als vorbereitende Maßnahme für einen mittelfristig geplanten Umzug selbst gehosteter Dienste zu einem DLZ-IT dienen.

#### 4.2.5.4.1 Einhaltung offener Standards

Insbesondere der letzte Punkt verdeutlicht, dass Standards für den Austausch virtueller Maschinen an Bedeutung gewinnen. Daher sollten bei der Planung künftiger virtueller Systeme neue Abhängigkeiten von Produkten und deren Herstellern (Vendor Lock-In) vermieden werden. Zwar sind offene Standards im Bereich der Virtualisierung noch rar (s. 4.2.5.1.6), doch die wenigen vorhandenen sollten bei der Auswahl der Virtualisierungslösung entsprechendes Gewicht erhalten. Zudem sollten nur solche Lösungen gewählt werden, die die o.g. häufigsten Formate für virtuelle Festplatten nativ unterstützen oder über geeignete Konverter für den Im- und Export dieser Formate verfügen. Vorhandene Virtualisierungslösungen und deren aktuelle Versionen sollten ebenfalls auf diese Kriterien überprüft und ggf. deren Ablösung durch besser unterstützende Lösungen in Betracht gezogen werden.

#### 4.2.5.4.2 Vermeiden unerwünschter Abhängigkeiten

Neben ungewollter Abhängigkeit über proprietäre Formate und Protokolle einer Virtualisierungslösung sollte auch die Abhängigkeit von einer proprietären Plattform oder bestimmter Hardware vermieden werden. Ausschließlich auf proprietären Wirtssystemen[56] oder Prozessoren einzelner Herrsteller[57] lauffähige Lösungen werden daher ebenso wenig betrachtet wie sonstige Lösungen mit ähnlich eng definierter Systemumgebung.

#### 4.2.5.4.3 Verwaltung

Wird ein größerer Bedarf an virtualisierten Systemen festgestellt, kommen deren Verwaltung durch zentrale IT-Abteilungen und die Erstellung und Nutzung von Vorlagen in Betracht. Die Virtualisierungslösungen sollten sowohl Werkzeuge für eine komfortable Verwaltung vieler virtueller Maschinen als auch für die konfliktfreie Instanziierung neuer virtueller Maschinen anhand von Vorlagen bieten. Dabei sollte es hinsichtlich der Server- und der Desktop-Virtualisierung möglich sein, virtuelle Maschinen zur Laufzeit auf ein anderes Wirtssystem zu verschieben. Auch sollten mehrere Instanzen derselben Vorlage parallel betrieben werden können, ohne die Resourcen der Wirtssysteme dabei im vollen nominellen Umfang zu belasten, indem beispielsweise identische Hauptspeicherbereiche nur einmal vorgehalten werden.

#### 4.2.5.4.4 Unterstützung lokaler Geräte

Bei der Desktop-Virtualisierung gilt es zu beachten, ob komplette Arbeitsplätze oder lediglich Teilsysteme wie einzelne Fachanwendungen virtualisiert werden sollen. Letzteres wird in Abgrenzung zur VDI als Anwendungs-Virtualisierung bezeichnet, bei der eine möglichst nahtlose Integration in die sonstige lokale Arbeitsumgebung notwendig ist. In beiden Fällen muss geprüft werden, welche lokalen Geräte – vom Kartenleser über Drucker und Smartphones bis zur Kamera für Videokonferenzen – im virtualisierten Desktop genutzt werden sollen und können. Hierfür sollten Tests unter repräsentativen Bedingungen durchgeführt werden.

[56] Beispielsweise Microsoft Hyper-V, das einen Microsoft Windows Server 2008 voraussetzt.
[57] Beispielsweise Citrix XenClient, der derzeit Intel-Prozessoren voraussetzt.

#### 4.2.5.4.5 Lizenzen

Auch beim Betrieb von Anwendungen oder Betriebssystemen innerhalb einer virtuellen Maschine sind die jeweiligen Lizenzbedingungen einzuhalten. Während OSS-Lizenzen den Betrieb sowohl in einer physikalischen als auch einer virtuellen Umgebung erlauben, kann es im proprietären Bereich Einschränkungen geben oder eine explizite Lizenz für virtuelle Umgebungen verlangt sein. Daher muss vor der Virtualisierung von (Teil-)Systemen jedes betroffene Produkt dahingehend untersucht werden, ob die vorhandenen Lizenzen den Betrieb in einer virtuellen Umgebung abdecken oder ggf. entsprechende Lizenzen beschafft werden müssen.

### 4.2.5.5 Produktauswahl

Eine empirisch fundierte Produktauswahl anhand der tatsächlichen Verbreitung ist im Kontext von Virtualisierungslösungen nicht möglich. Weder existieren hierzu repräsentative Umfragen, noch eignen sich dazu allein die Verkaufszahlen einzelner Hersteller, weil Open-Source-Lösungen frei zur Verfügung stehen und dabei unbeachtet blieben. Die jeweilige Produktauswahl basiert daher auf Schätzungen.

#### 4.2.5.5.1 Server-Virtualisierung

Für eine Server-Virtualisierung sind Technologie und Leistungsfähigkeit des jeweiligen Hypervisors maßgebend für den erfolgreichen Einsatz einer Gesamtlösung. Er ist damit der Kernbestandteil jeder Virtualisierungslösung und steht im Mittelpunkt der Produktauswahl und -bewertung. Die dazu jeweils verfügbaren Hilfsmittel werden punktuell in der Bewertung hinzugezogen. Für die Server-Virtualisierung werden folgende Hypervisor in der jeweils aktuellen Version betrachtet:

- **VMware vSphere Hypervisor** des Marktführers VMware,
- **Xen Hypervisor** als bei Behörden verbreiteter Hypervisor sowie
- **KVM** als führender OSS-Hypervisor.

#### 4.2.5.5.2 Desktop-Virtualisierung

Bei der Desktop-Virtualisierung stehen teils andere Aspekte wie Zugriffsprotokolle, Trennung von Standard-Desktop und Anwenderdaten und resourcenschonender Parallelbetrieb vieler gleichartiger Desktops im Vordergrund. Die Produktauswahl unterscheidet sich daher von derjenigen für die Server-Virtualisierung, es werden folgende Produkte in der jeweils aktuellen Version betrachtet:

- **VMware View** des Marktführers VMware,
- **UCS Desktop Virtualization Services** als Teil des bei Behörden verbreiteten Univention Corporate Servers sowie
- **Red Hat Enterprise Virtualization for Desktops** als einem führenden OSS-Produkt.

#### 4.2.5.5.3 Anwendungs-Virtualisierung

Die Anwendungs-Virtualisierung hat wiederum einen anderen Fokus als die beiden vorgenannten Virtualisierungsarten. Hier steht die Nutzung von virtualisierten Anwendungen auf dem lokalen Arbeitsplatzrechner möglichst ohne Auswirkungen auf denselben im Vordergrund. Der Anwender soll sie so transparent nutzen können, wie es eine lokale Installation ermöglichen würde.

Derzeit werden unter dem Stichwort der Anwendungs-Virtualisierung lediglich Lösungen angeboten, die die Paketierung Windows-basierter Anwendungen und deren Ausführung in einer gesicherten Umgebung (Sandbox) wiederum auf einer Windows-Plattform beinhalten. Dies gilt insbesondere für die Produkte

- Citrix XenApp,

- Microsoft Application Virtualization (App-V),
- VMware ThinApp (ehemals jitit Thinstall),
- Novell ZENworks Application Virtualization,
- Symantec Endpoint Virtualization Suite (ehemals Altiris SVS),
- Sandboxie,
- Evalaze,
- Cameyo und
- Ceedo.

Diesen Produkten liegen keine offenen Standards für die Paketierung oder deren geschützter Ausführung zugrunde. Auch können sie nicht auf alternativen Plattformen genutzt werden. Der Begriff Anwendungs-Virtualisierung ist für deren Einsatzzweck zu ungenau. Diese Produkte werden daher im weiteren Text unter *Windows-Sandboxes* zusammengefasst und nicht weiter betrachtet.

Alternativ zu diesem stark Plattform-fokussierten Ansatz existieren Produkte für eine lokale Desktop-Virtualisierung, bei der ein lokaler Hypervisor dazu genutzt wird, lokal verfügbare virtuelle Maschinen auszuführen. Diese Produkte können auch für die Virtualisierung einzelner Anwendungen verwendet werden und bieten eine regelmäßig eine gute Integration in den lokalen Desktop. Zwar ist dazu die Installation eines Hypervisors auf dem jeweiligen Arbeitsplatzrechner (APC) notwendig, doch der Betrieb von Anwendungen in einer lokalen virtuellen Maschine hat keine sonstigen Änderungen am APC zur Folge. Aus dieser Gruppe werden folgende Produkte in der jeweils aktuellen Version betrachtet:

- **VMware Workstation** des Marktführers VMware,
- **Oracle VirtualBox** als einer bei Behörden verbreiteten und zudem führenden OSS-Lösung und
- **Parallels Desktop** als der führenden Lösung für das MacOS X.

#### 4.2.5.6 Bewertung

In die Bewertung fließen die Beherrschung der jeweiligen Grundfunktionalität und Hilfsmittel zur Verwaltung ebenso ein wie Metainformationen zu Lizenzen und sonstigen Einschränkungen. Angesichts der sehr vielen Aspekte des Themas Virtualisierung wird je Typ nur auf die hinsichtlich einer Migration relevantesten eingegangen.

##### 4.2.5.6.1 Server-Virtualisierung

**VMware** stellt als Marktführer eine breite Palette an Virtualisierungsprodukten und unterstützenden Werkzeugen bereit. Das hier betrachtete vSphere richtet sich an Großkunden wie Rechenzentren und bietet für alle Aspekte der Server-Virtualisierung angemessene Lösungen in modularer Form, angefangen vom kostenlos nutzbaren Typ 1-Hypervisor (siehe 4.2.5.1.2) über Konvertierungshilfen und Monitoring bis hin zu Verwaltungswerkzeugen für die private Cloud.

VMware unterstützt mit OVF den offenen Standard für den Austausch von virtuellen Maschinen und -kombinationen und ist u.a. im Rahmen der DMTF an der Fortentwicklung offener Standards für die Verwaltung virtueller Systeme beteiligt. Allerdings stellt VMware keines seiner relevanten Produkte unter eine OSS-Lizenz, sondern verlangt vielmehr Lizenzgebühren im Enterprise-Maßstab. Die Berechnungsbasis der Lizenzgebühren anhand des virtuellen Arbeitsspeichers (vRam) je Prozessor ist nachvollziehbar, ein Verschieben der virtuellen Kapazitäten innerhalb des lizenzierten Rahmens möglich.

Mit dem vSphere Hypervisor stellt VMware ein kostenloses Einstiegspaket bereit, welches bei Gefallen kostenpflichtig um weitere Komponenten aus dem vSphere/ESXi-Umfeld ergänzt werden kann.

Als „bare metal“-Hypervisor müssen beim Einsatz des vSphere Hypervisor keine Wirtssysteme beachtet werden, bei den möglichen Gastsystemen gibt es keine nennenswerten Einschränkungen. Die verfügba-

ren Verwaltungswerkzeuge sind ausgereift und ermöglichen u.a. die Integration der virtuellen Maschinen in vorhandene Verzeichnisdienste wie LDAP und AD.

Soll von früheren VMware-Produkten auf die aktuelle Palette migriert werden, ist das seit jeher verwendete VMDK-Format für virtuelle Festplatten eine gute Voraussetzung für eine erfolgreiche Migration, die sich dadurch auf die korrekte Umschreibung der Metadaten wie Prozessortyp, Blockdevice-Controller oder Netzwerkverbindung konzentrieren kann.

**XEN** als erster OSS-Hypervisor hat im Enterprise-Umfeld weite Verbreitung gefunden, insbesondere durch die im Vergleich zur Emulation sehr schnelle Ausführungsgeschwindigkeit von Gastsystemen durch das Prinzip der Paravirtualisierung. XEN ist ein Typ 1-Hypervisor und weist neben der allen untersuchten Hypervisoren gemeinsamen transparenten Paravirtualisierung zudem die einzigartige Fähigkeit auf, einzelne Hardware-Komponenten an bestimmte Gastsysteme durchzureichen. Dadurch können ggf. spezifische Performance-Probleme behoben werden. Allerdings ist diese Fähigkeit bei der Server-Virtualisierung nur in wenigen Fällen sinnvoll einsetzbar und behindert zudem das Verschieben virtueller Maschinen auf andere Wirtssysteme.

XEN ist als einziger betrachteter Hypervisor auch ohne vorhandene Hardware-Unterstützung in der Lage, Gastsysteme paravirtualisiert zu betreiben. Dies erfordert aber die Anpassung der Gastsysteme, Microsoft Windows Server 2008 R2 kann in diesem Fall nicht als Gastsystem genutzt werden.

Eine Migration früherer XEN-Installationen und darauf basierender virtueller Maschinen („Domänen“ im XEN-Jargon) auf aktuelle Versionen sollte aufgrund des fortbestehenden VHD-Formats analog zu VMware ohne größere Probleme möglich sein.

Mit Citrix übernahm eine Firma mit vieljähriger Erfahrung in Windows-Terminallösungen die ursprünglich hinter XEN stehende Firma XenSource und treibt die Entwicklung XEN-basierter Lösungen für das Enterprise-Umfeld voran. Der Hypervisor selbst steht unter der OSS-Lizenz GPL v2 und ist nach Jahren der Annäherung 2011 in den Linux-Kernel aufgenommen worden. Citrix bietet auf dessen Basis ein breites Portfolio an Verwaltungs- und sonstigen Werkzeugen an, die allerdings proprietärer Natur sind und nach Bedarf lizenziert werden können.

Im Gegensatz zu VMware setzt Citrix stark auf Microsoft-Plattformen. Das zentrale Verwaltungswerkzeug XenCenter und viele weitere Hilfsmittel gibt es nur in einer Windows-Version, und auch der Im-/Export von OVF-Dateien gelingt nur auf der Basis von .NET. Der ursprüngliche OSS-Charakter von XEN geht mit den darauf basierenden Citrix-Produkten zunehmend verloren. Auch schwindet trotz Aufnahme in den Linux-Kernel die Unterstützung des Hypervisors durch führende Linux-Distributoren zugunsten von KVM.

**KVM** ist der jüngste OSS-Hypervisor und im Gegensatz zu den vorgenannten Produkten vom Typ 2, kommt also ohne eigene Hardware-Treiber aus. Er ist vielmehr eine Erweiterung des Linux-Kernels um die Fähigkeit zum Betrieb virtueller Gastsysteme und nutzt dessen Fähigkeiten und die des langerprobten Emulators QEMU geschickt aus, was ihm inzwischen die Unterstützung aller namhaften Linux-Distributionen einbrachte.

KVM wurde 2006 veröffentlicht und nur wenige Monate später in den Linux-Kernel aufgenommen. Dadurch blieb ihm das für XEN jahrelang notwendige Pflegen eigener Kernelversionen erspart. Er gewann schnell die Aufmerksamkeit der Prozessorhersteller Intel und AMD, mit deren Hilfe KVM in kurzer Zeit die Performance-Werte hergebrachter Hypervisoren erreichen konnte. KVM wurde ursprünglich von der Firma Qumranet entwickelt, die 2008 von Red Hat gekauft wurde. Red Hat steht gemeinsam mit HP, IBM, Intel und weiteren Firmen hinter der 2011 gegründeten Open Virtualization Alliance mit dem Ziel, dem Einsatz von KVM und darauf basierenden Produkten den Weg zu ebnen.

KVM nutzt die inzwischen regelmäßig vorhandene Hardwareunterstützung durch AMD-V und Intel VT-x und erreicht auf dieser Basis ähnlich gute Performance-Werte wie die vorgenannten „bare metal“-Hypervisor. Beim Fehlen derselben greift er alternativ auf den Voll-Emulator QEMU zurück, was naturgemäß mit deutlichen Performance-Einbußen verbunden und daher nicht empfehlenswert ist. Mit KVM

ist der Betrieb diverser Gastsysteme (u.a. Windows Server 2008 und Linux) auf sehr vielen Hardware-Plattformen möglich. Er unterstützt verschiedene Formate für virtuelle Maschinen, u.a. das verbreitete VMDK; die Konvertierung weiterer Formate in unterstützte und der Im- und Export von OVF-Dateien gelingen mit verschiedenen Werkzeugen aus dem OSS-Umfeld.

Die Hypervisor KVM und XEN werden von einer Vielzahl an Verwaltungswerkzeugen unterstützt, deren Fokus von der lokalen Desktop- über die Server-Virtualisierung bis hin zum Cloud Computing reichen und oft auch noch weitere Hypervisor mit einbeziehen können. Viele dieser Verwaltungswerkzeuge sind wie die beiden Hypervisor ebenfalls OSS, die Offenheit im Bereich der Virtualisierung hat sich inzwischen etabliert.

Tabelle 4.6: Vergleich Server-Virtualisierung

| **Hypervisor** | **VMware vSphere** | **XEN** | **KVM** |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | – | ✓ | ✓ |
| Lizenzkosten | pro phys. CPU | – | – |
| Einschränkungen | max. 96GB vRAM/VM[58] | – | – |
| Unbeschränkte Anzahl Gastsysteme | ✓[59] | ✓ | ✓ |
| **Grundfunktionen** | | | |
| Hypervisor-Typ | Typ 1 | Typ 1 | Typ 2 |
| Benötigte Plattform | – | Anpassbares OS[60] | Linux |
| Unterstützte Gastsysteme (Windows Server 2008 R2 / Linux)[61] | ✓/✓ | ✓[62]/✓ | ✓/✓ |
| Unterstützung VM-Formate VMDK/VDI/VHD/QCOW[63] | ✓/–/✓[64]/– | ✓/–/✓/– | ✓/–/✓/✓ |
| **Resourcen-Optimierung** | | | |
| Durchreichen einzelner Geräte | – | ✓ | – |
| Explizite Paravirtualisierung | – | ✓ | – |
| Transparente Paravirtualisierung durch Nutzung von AMD-V oder Intel VT | ✓ | ✓ | ✓ |
| Hauptspeicher-Überbuchung[65] | ✓ | ✓ | ✓ |
| Gemeinsame Speicherbereiche[66] | ✓ | ✓ | ✓ |

[58] Je nach Lizenz, von vSphere Essentials über Standard bis Enterprise Plus. Für den kostenlosen VMware vSphere Hypervisor stehen max. 32GB vRAM auf Hosts mit beliebig vielen CPUs und max. 32GB phys. RAM zur Verfügung.
[59] Innerhalb der vRAM- und CPU-Grenzen der jeweiligen Lizenz, s. Zeile Einschränkungen.
[60] Als privilegiertes Gastsystem; anpassbar sind insbesondere OSS-Betriebssysteme wie Linux.
[61] Im Rahmen der Server-Virtualisierung werden nur Server-Betriebssysteme als Gäste betrachtet.
[62] Nur bei transparenter Paravirtualisierung
[63] VM-Formate jeweils mit fester und dynamischer Größe
[64] Konvertierung mittels VMware vCenter Converter
[65] Die Summe des virtuellen RAM aller VMs eines Servers übersteigt dessen physikalisches RAM und wird dynamisch zwischen den VMs verteilt.
[66] Speicherblöcke verschiedener VMs mit identischem Inhalt werden zu einem zusammengefasst.

| Hypervisor | VMware vSphere | XEN | KVM |
|---|---|---|---|
| **Verwaltung** | | | |
| VM-Verwaltung, Monitoring[67] | VMware vCenter Server, VMware Studio, OpenQRM | XenCenter, virt-manager, ConVirt, OpenQRM | virt-manager, Zentific, ConVirt, OpenQRM |
| Im-/Export von OVF-Paketen | ✓ | ✓[68] | (✓)[69] |
| Erstellen von Zwischenständen | ✓ | ✓ | ✓ |
| Live-Migration | ✓ | ✓ | ✓ |
| Individualisierte VM-Klone | ✓ | ✓ | ✓ |

**Empfehlungen:** Derzeitige Virtualisierungslösungen konzentrieren sich vorwiegend auf die verbreiteten x86/x64-Systeme und nutzen durchweg die seit einigen Jahren verfügbaren Prozessor-Erweiterungen zur Virtualisierungsunterstützung, namentlich AMD-V und Intel VT-x. Dadurch kann das Prinzip der Paravirtualisierung mit allen gängigen Gastsystemen genutzt werden und führt gegenüber voll emulierten Umgebungen zu deutlichen Geschwindigkeitsvorteilen. Bei der Beschaffung von Hardware sollte daher darauf geachtet werden, dass diese Unterstützung gegeben ist.

Ist mit einer Migration ein Wechsel des Hypervisors verbunden, muss geprüft werden, ob das bisherige Speicherformat der virtuellen Maschine auch vom künftigen Hypervisor unterstützt wird und beibehalten werden kann. Ist dies nicht der Fall, können mit dem freien Konverter qemu-img alle gängigen VM-Formate im- und exportiert werden. In den Gastsystemen vorhandene Hypervisor-Spezifika wie spezielle Treiber sollten auf Verträglichkeit mit dem künftigen Hypervisor geprüft und ggf. vor dem Wechsel des Hypervisors entfernt werden, da sie sonst den Start der virtuellen Maschine unter dem neuen Hypervisor behindern können. Auch sollte insbesondere bei älteren Gastsystemen geprüft werden, ob die bisher emulierte Umgebung (Systemarchitektur, Chipsatz, ...) vom künftigen Hypervisor adäquat bereitgestellt werden kann.

VMware ist seit den Anfängen der x86-Virtualisierung mit Produkten am Markt und verfügt über entsprechend viel Erfahrung, was sich an seinen durchweg ausgereiften Produkten zeigt. Der Anbieter ist an offenen Standards und deren Umsetzung interessiert und beteiligt sich an entsprechenden Gremien. Auch wenn keine Komponenten unter OSS-Lizenzen bereitgestellt werden, ist vSphere für die Server-Virtualisierung eine sinnvolle Alternative und kann mit dem Einstiegspaket kostenlos ausprobiert werden.

Der XEN-Hypervisor sollte vor allem dann näher betrachtet werden, wenn mangels Hardware-Unterstützung seine Fähigkeiten zur expliziten Paravirtualisierung von Vorteil sind oder einzelne Hardware-Komponenten an bestimmte Gastsysteme durchgereicht werden sollen. Da er auf ein privilegiertes Gastsystem angewiesen ist, gestaltet sich das Aufsetzen einer Server-Virtualisierung vergleichsweise komplex. Ein Rückgriff auf XEN-basierte Produkte des Citrix-Portfolios erspart zwar entsprechend höhere Aufwände, bringt aber bei zentralen Komponenten Abhängigkeiten zu Microsoft-Produkten mit sich. Alternativ stehen diverse OSS-Werkzeuge und -Produktportfolios bereit, mit denen eine XEN-basierte Server-Virtualisierung gut gelingen kann und die auch kommerziellen Support anbieten. Angesichts der schwindenden Unterstützung durch führende Linux-Distributoren zugunsten von KVM ist die Zukunft des XEN-Hypervisor aber eher ungewiss.

[67] Es werden beispielhaft verbreitete Produkte aufgeführt, weitere Alternativen sind vorhanden.
[68] Nur unter Windows mittels Project Kensho
[69] OVF-Import über virt-convert

KVM hingegen ist auf dem besten Weg, der verbreitetste OSS-Hypervisor zu werden, und verfügt mit den in der Open Virtualization Alliance versammelten IT-Schwergewichten über eine starke Unterstützung. Durch die Installation von KVM als Linux-Kernelmodul und des virt-manager als Verwaltungswerkzeug ist das Aufsetzen einer Virtualisierungslösung für kleine und mittlere Behörden vergleichsweise trivial. Die meisten OSS-Werkzeuge im Bereich der Virtualisierung unterstützen die Hypervisor XEN und KVM gleichermaßen und stellen weitergehende Verwaltungshilfen bereit, mit denen auch komplexere Systeme großer Behörden oder Rechenzentren bewältigt werden können. Aufgrund seiner hervorragenden Linux-Integration und der breiten Unterstützung ist eine hohe Investitionssicherheit wahrscheinlich und die Auswahl an kommerziellen Dienstleistungen vielfältig. KVM ist daher eine sinnvolle Alternative für die Server-Virtualisierung.

#### 4.2.5.6.2 Desktop-Virtualisierung

**VMware View** ist eine Komplettlösung[70] für die Desktop-Virtualisierung in Microsoft-dominierten Gesamtsystemen. Als Endgeräte können Standard-PCs mit verschiedenen Windows-Plattformen ab XP SP3 und installiertem VMware View Client oder von VMware dafür zertifizierte Zero-Clients[71] eingesetzt werden. Über das von Teradici entwickelte proprietäre Zugriffsprotokoll PCoIP können die Endgeräte neben den üblichen Steuerungsmöglichkeiten entfernter virtueller Maschinen (Maus, Tastatur, Bildschirm) mehrere Monitore, Video- und Audio-Streaming sowie diverse lokale USB-Geräte nutzen.

Der VMware View Manager sorgt in Verbindung mit weiteren Komponenten für gesicherte Datenverbindungen und kann beliebig vielen Anwendersitzungen ein identisches Grundsystem mit den jeweils spezifischen Daten und Einstellungen bereitstellen. Er benötigt zur Laufzeit ein Microsoft Active Directory. Der Offline-Betrieb virtueller Maschinen und deren Abgleich mit dem Grundsystem bei bestehender Netzverbindung ist ebenso möglich wie die zentrale Aktualisierung und Verteilung des Grundsystems im laufenden Betrieb.

VMware View unterstützt das vDesktop-Pooling, bei dem virtuelle Maschinen nach der Abmeldung eines Benutzers weiterlaufen und mit dem nächsten Anmelder verbunden werden können. Zudem können laufende virtuelle Maschinen je nach Gesamtauslastung auf wenige Wirtssysteme zusammengezogen werden, um die frei werdenden Wirtssysteme in einen Energiesparmodus versetzen zu können. Abbilder von VM-Vorlagen werden mit der Vorlage so verlinkt, dass nur wenig zusätzlicher Plattenplatz pro vDesktop benötigt wird.

Als Laufzeitumgebung für Nicht-Windows-Endgeräte hat VMware den VMware View Open Client unter der LGPL[72] freigegeben. Dieser verfügt allerdings nur über rudimentäre Fähigkeiten, die Nutzung des proprietären Protokolls PCoIP und von lokalen USB-Geräten ist beispielsweise nicht möglich. Die übrigen Komponenten von VMware View sind proprietär und mit Lizenzkosten im für Großkunden und Rechenzentren üblichen Maßstab verbunden.

**Die UCS Desktop Virtualization Services (UCS DVS)** sind ein optionaler Aufsatz auf den Univention Corporate Server für die Virtualisierung von Windows- und Linux-Desktops. Explizit unterstützt werden als Gastsysteme Windows XP und 7 sowie der hauseigene Univention Corporate Desktop. Darauf zugegriffen werden kann über einen nativen DVS-Client unter Windows und Linux oder mit Thin Clients, für die auch eine Multi-Monitor-Anbindung möglich ist. Audio-Streaming klappt mit allen Varianten, Video-Streaming nur für Windows-Gäste.

UCS DVS verwaltet die aktiven Verbindungen zwischen den virtuellen Desktops und den per DVS-Client angemeldeten Anwendern über einen Session Manager und setzt auf dem UCS Virtual Machine Manager (UVMM) auf, der Grundfunktionen zur Verwaltung virtueller Maschinen bereitstellt, beispielsweise die Live-Migration oder das Generieren neuer Instanzen virtueller Maschinen anhand entsprechender Vorlagen. Er stellt auch einen VNC-Zugriff auf die virtuellen Desktops bereit. Über

[70] In der Version VMware View 4.5 Premier Starter Kit

[71] Die Zero-Clients werden mit fest installierter Zugriffssoftware für VMware View ohne Anpassungsmöglichkeit ausgeliefert.

[72] Die LGPL ist eine verbreitete OSS-Lizenz; für weitere Informationen siehe 3.4.1.

das UCS-Identitymanagement lässt sich DVS in AD- und LDAP-Umgebungen integrieren. Der Offline-Betrieb virtueller Desktops ist ebenso wenig möglich wie die zentralisierte Aktualisierung von Standard-Plattformen, der Im- und Export von OVF-Paketen wird nicht unterstützt.

Beim Klonen von VMs werden nur Änderungen zur Vorlage gespeichert (Copy-on-Write), was der Einsparung von Plattenplatz dient. Für kommende Versionen von DVS sind das vDesktop-Pooling und das energieeffiziente Vorhalten virtueller Maschinen auf wenigen Wirtssystemen geplant.

Univention stellt den Quellcode aller an seiner Lösung beteiligten Komponenten unter OSS-Lizenzen zur Verfügung. Mit einer zweiten Lizenz für das „Gesamtwerk“ und dessen geschäftsmäßigem Einsatz werden dennoch Lizenzgebühren fällig, die allerdings deutlich unter denen von VMware liegen und mit einer Zielgröße von 50 - 500 vDesktops auf einen Einsatz in kleinen bis mittelgroßen Behörden und Firmen zielen.

**Red Hat Enterprise Virtualization for Desktops (RHEVD)** ist eine weitere OSS-basierte Lösung mit einer zweiten Lizenz für den geschäftsmäßigen Einsatz, die hinsichtlich der Lizenzkosten zwischen den Alternativen von VMware und Univention liegt.

Mit SPICE forciert Red Hat den Einsatz eines neuen, quelloffenen Protokolls mit dem Ziel, die an der Virtualisierung beteiligten Hardware-Resourcen bezüglich der Netzwerk-Bandbreite und des Grafik-Renderings möglichst optimal zu nutzen. Dessen Implementierung erlaubt neben den üblichen Steuerungsmöglichkeiten Audio- und Video-Streaming, die Anbindung mehrerer Monitore an eine virtuelle Maschine und die Nutzung lokaler USB-Geräte. Red Hat stellt sogenannte SPICE Clients als Firefox-Plug-In und ActiveX-Control für den Microsoft Internet Explorer zur Verfügung. Da solche Browser-Erweiterungen nicht überall zulässig sind, können alternativ die Protokolle RDP und RFB/VNC genutzt werden.

RHEVD unterstützt alle betrachteten Client-Plattformen und als Gastsysteme Windows und Linux. Letztere können durchweg lokale USB-Geräte, Video- und Audio-Streaming nutzen und mit mehreren Monitoren verbunden werden.

Der Red Hat Enterprise Virtualization Manager dient zur Verwaltung der virtuellen Desktops. Mit dem integrierten Connection Broker werden Verbindungen zwischen den gepoolten vDesktops und den Anwendern hergestellt. Auch diese Lösung spart physikalischen Plattenplatz durch geschicktes Verknüpfen der VM-Vorlage mit dem jeweiligen vDesktop. Die Live-Migration virtueller Maschinen ist ebenso möglich wie das Erstellen von Zwischenständen, und auch der Im- und Export von OVF-Paketen wird unterstützt.

Tabelle 4.7: Vergleich Desktop-Virtualisierung

| Produkt | VMware View | UCS DVS | RHEVD |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | – | ✓ | ✓ |
| Lizenzkosten | pro 10 vDesktops[73] | pro vDesktop | pro 25 vDesktops |
| Notwendige Infrastruktur | VMware vSphere | Univention Corporate Server | Red Hat Enterprise Linux[74] |
| Hypervisor | VMware vSphere | XEN, KVM | KVM |
| Einschränkungen | s. vSphere-Bewertung | – | pro Host und Gast[75] |

[73] Bei der Berechnung der Lizenzkosten sind gleichzeitig genutzte virtuelle Desktops (vDesktop) maßgebend.
[74] Oder auf die Virtualisierung spezialisierte RHEL-Varianten.
[75] Pro Host max. 96 phys. CPUs und 1 TB RAM. Pro Gast max. 16 vCPUs und 256 GB vRAM.

| Produkt | VMware View | UCS DVS | RHEVD |
|---|---|---|---|
| **Grundfunktionen** | | | |
| Unterstützte Gast-Plattformen<br>Windows XP/7/Linux/MacOS X | ✓/✓/✓/✓ | ✓/✓/✓[76]/– | ✓/✓/✓[77]/– |
| Unterstützte Client-Plattformen<br>Windows XP/7/Linux/MacOS X | ✓/✓/–/✓ | ✓/✓/✓/–[78] | ✓/✓/✓/✓ |
| Client-Runtime | VMware View Client, VMware View Open Client, Thin („Zero“) Client | Nativer DVS-Client, Thin Client[79] | Webbrowser mit SPICE-Plug-In/-ActiveX, Thin Client[80] |
| Zugriffs-Protokolle | VNC, RDP, PCoIP | VNC, RDP, x2go | VNC, RDP, SPICE |
| Offline-Fähigkeit | ✓ | – | – |
| Nutzung lokaler USB-Geräte | ✓ | ✓[81] | ✓ |
| Medien-Unterstützung<br>Video-/Audiostreaming/Mehrere Monitore | ✓/✓/✓ | ✓[82]/✓/✓[83] | ✓/✓/✓ |
| **Resourcen-Optimierung** | | | |
| Getrennte Nutzerdaten | ✓ | ✓ | ✓ |
| Reduzierter Plattenplatz | ✓(Linked Clone) | ✓(Copy-on-write) | ✓(Linked Image) |
| vDesktop-Pooling | ✓ | –[84] | ✓ |
| Grafik-Rendering auf Client | – | – | ✓ |
| **Verwaltung** | | | |
| Notwendige Middleware | VMware View Manager, VMware vCenter Server | UCS Virtual Machine Manager (UVMM) | Red Hat Enterprise Virtualization connection broker |
| Im-/Export von OVF-Paketen | ✓ | – | ✓ |
| Erstellen von Zwischenständen | ✓ | ✓[85] | ✓ |
| Live-Migration | ✓ | ✓ | ✓ |
| Individualisierte VM-Klone | ✓ | ✓ | ✓ |

**Empfehlungen:** Zwar bietet VMware mit View eine auf den ersten Blick vollständige Lösung für die Desktop-Virtualisierung an. Doch trifft dies nur für Windows-basierte oder unveränderliche Endgeräte

[76] Explizit unterstützt wird der Univention Corporate Desktop
[77] Explizit unterstützt wird der Red Hat Enterprise Desktop
[78] Ein nativer DVS-Client für MacOS X ist geplant.
[79] in Kombination mit UCS Thin Client Services
[80] in Kombination mit SPICE Client
[81] Über RDP. Die Nutzung lokaler USB-Geräte durch über x2go angesprochene Linux-Gäste ist geplant.
[82] Über RDP, derzeit nur für Windows-Gäste
[83] Nur für Thin Clients
[84] Geplant
[85] Beim Einsatz von KVM als Hypervisor. Das Erstellen von Zwischenständen beim Einsatz von XEN ist geplant.

zu, und auch die zentralen Verwaltungskomponenten schaffen mit AD unerwünschte Abhängigkeiten. Aufgrund der Ausrichtung auf proprietäre Plattformen und Protokolle kann VMware View daher derzeit für die Migration zu offenen Standards im Bereich der Deskop-Virtualisierung nicht empfohlen werden.

Univention hingegen stellt alle Komponenten seiner VDI-Lösung unter OSS-Lizenzen bereit und lässt dadurch den Mangel an offenen Standards in diesem Bereich weniger gravierend erscheinen. Zudem hat der Käufer die Wahl zwischen den Hypervisors KVM und XEN. Allerdings sind die Grundfunktionen der Lösung noch ausbaufähig, und auch die Resourcen-Optimierung befindet sich großteils noch im Stadium der Planung. Angesichts der Politik der Offenheit und der Unterstützung verschiedener Plattformen und Verzeichnisdienste ist eine eingehendere Prüfung dieser Lösung aber trotzdem sinnvoll, insbesondere für kleine und mittlere Behörden.

Die Alternative von Red Hat basiert ebenfalls auf OSS-Paketen und kann über den Umweg CentOS sogar kostenfrei bezogen werden, dann allerdings ohne jeden Support von Red Hat. Sie überzeugt durch eine recht vollständige Abdeckung der untersuchten Kriterien und bietet eine auf Großkunden ausgelegte Infrastruktur. Mit SPICE wird zudem ein interessanter Gegenentwurf zum von VMware propagierten proprietären PCoIP-Protokoll eingeführt. Als Marktführer bei kommerziellen Linux-Distributionen verfügt Red Hat über die nötige Erfahrung im Umgang mit und Support von Großkunden. Insbesondere große Behörden sollten diese VDI-Lösung daher näher prüfen und auf die eigenen Bedürfnisse hin untersuchen.

#### 4.2.5.6.3 Anwendungs-Virtualisierung

**VMware Workstation** bringt alle wichtigen Eigenschaften zur lokalen Virtualisierung von Windows- oder Linux-Gastsystemen unter Windows- oder Linux-Wirten mit. MacOS X wird weder als Wirts- noch als Gastsystem unterstützt, obwohl der MacOS X Server die Verwendung in einer virtuellen Umgebung erlaubt. Dafür weist VMware Workstation mit der treiberlosen Druckerverwendung in Gastsystemen ein Alleinstellungsmerkmal auf.

Die Konfiguration neuer virtueller Maschinen gelingt mithilfe vorkonfigurierter Einstellungen für gebräuchliche Gastsysteme schnell. Für die Virtualisierung eines physikalisch installierten Systems bietet VMware mit dem vCenter Converter ein kostenloses Hilfsmittel an. Wie bei VMware üblich handelt es sich auch bei der VMware Workstation um proprietäre Software, für die Lizenzen erworben werden müssen. Die Einschränkungen hinsichtlich der maximalen Anzahl virtueller CPUs und der Hauptspeichergröße sind für den lokalen Desktop-Betrieb nicht weiter hinderlich. Für die fehlende USB-3.0-Unterstützung gilt derzeit dasselbe.

Mit OVF unterstützt VMware Workstation den offenen Standard für den Austausch virtueller Maschinen. Soll die lokale Virtualisierungslösung auch entfernt genutzt werden, setzt VMware hierfür auf das offene Protokoll RFB/VNC. Virtuelle Maschinen werden im freien hauseigenen VMDK-Format abgelegt.

Das Verwalten verschiedener virtueller Maschinen mit VMware Workstation ist ebenso möglich wie das Erstellen und Wiederherstellen von Zwischenständen. Die Integration virtueller Maschinen in den lokalen Desktop ist umfänglich gelöst, im *Unity Mode* verschwinden die Grenzen zwischen Wirts- und Gastsystem weitgehend.

**Oracle VirtualBox** steht für alle betrachteten Gast- und Wirtssysteme mit jeweils gleichem Funktionsumfang zur Verfügung. Virtuelle Maschinen können bequem verwaltet, geklont und Zwischenstände gesichert und wieder hergestellt werden. Die VirtualBox beherrscht den Im- und Export von OVF-Paketen, unterstützt die Formate VMDK und VHD voll und Virtual Hard Disk Drive (HDD) teilweise. Sie bietet eine detaillierte und je nach Gastsystem vorbelegte Konfiguration virtueller Maschinen. Mit dem Kommandozeilen-Werkzeug VBoxManage lässt sich das Abbild einer physikalischen Installation[86] zu einer virtuellen Maschine wandeln, die im offenen Format VDI abgelegt wird.

[86] Abbilder physikalischer Installationen können bspw. mit dd erstellt werden.

Oracle VirtualBox ist aufgeteilt in ein Grundsystem unter der OSS-Lizenz GPL v2 und derzeit einem Erweiterungspaket unter der *Personal Use and Evaluation License (PUEL)*. Letzteres bringt USB-2.0-Support, Fernsteuerung per RDP und PXE zum Booten über das Netzwerk, ist allerdings über den persönlichen Gebrauch hinaus lizenzpflichtig. Die Einschränkung auf max. 32 CPUs in einer virtuellen Maschine ist eher theoretischer Natur; interessant hingegen ist die Möglichkeit zur Begrenzung der jeder virtuellen CPU zur Verfügung stehenden Zeit auf einer physikalischen CPU. Damit können alle physikalischen CPUs einem Gastsystem zugewiesen werden, ohne ersteres bei Vollast des Gastes zu blockieren.

Die Integration in das Wirtssystem gelingt weitgehend, mit dem *Seamless Mode* können einzelne Gastanwendungen wie lokal installierte verwendet werden. Drag&Drop zwischen Wirt und Gast wird allerdings nicht unterstützt, und am Wirt angeschlossene Drucker müssen als Netzwerkdrucker konfiguriert und mit Treibern versehen werden. Die Verwendung mehrerer Monitore im Gastsystem ist möglich, 2D- und 3D-Beschleunigung kann zugeschaltet und für die Audio-Unterstützung aus verschiedenen virtuellen Hardware-Komponenten die gewünschte ausgewählt werden.

**Parallels Desktop** richtet sich vorrangig an die Nutzer von MacOS X-Systemen, um ihnen den virtuellen Betrieb von Windows- und Linux-Gästen zu ermöglichen. Eine Version für Windows und Linux als Wirtssysteme wird ebenfalls angeboten, hinkt der aktuellen Mac-Version jedoch deutlich hinterher. Die Verwaltung virtueller Maschinen beinhaltet alle relevanten Funktionen, Snapshots können erstellt und restauriert werden. Virtuelle Maschinen in den Formaten VMDK, VDI und VHD können in das ausschließlich betreibbare proprietäre Format HDD konvertiert werden, und mit Parallels Transporter steht ein Werkzeug zur Virtualisierung einer physikalischen Installation bereit. Der Im- und Export von OVF-Paketen wird hingegen nicht unterstützt.

Parallels Desktop verfolgt wie die beiden vorgenannten Alternativen den Ansatz einer möglichst vollständigen Integration von Gast-Anwendungen in den Wirts-Betrieb, was für Windows-Gäste unter MacOS X als Wirt auch sehr gut gelingt. Die nahtlose Integration (hier Coherence genannt) bringt eine weitgehende Angleichung von Aussehen und Verhalten der Windows-Gastapplikation zu nativen MacOS-Programmen und ermöglicht Drag&Drop zwischen Wirt und Gast. Für Linux-Gäste ist beides nicht verfügbar, aber immerhin ein gemeinsames Clipboard und gemeinsame Ordner. An den Wirt angeschlossene Drucker müssen explizit im Gastsystem installiert werden. Der Betrieb mehrerer Monitore durch das Gastsystem ist möglich, Audio-Unterstützung vorhanden, 2D- und 3D-Beschleunigung kann zugeschaltet werden.

Parallels Desktop ist eine proprietäre Software, die lizenziert werden muss. Die Resourcen für einzelne virtuelle Maschinen sind zwar teils stärker beschränkt als bei den Konkurrenten, doch lassen sie für die lokale Desktop-Virtualisierung derzeit immer noch genügend Raum. Beim Erstellen virtueller Maschinen werden je nach Gast Konfigurationen vorgeschlagen. Die Auswahl der virtuellen Basis-Hardware ist teils fest vorgegeben, teils nur grob einstellbar. Das erleichtert zwar dem unbedarften Anwender die Arbeit, kann aber beim Import fremder VMs zu Inkompatibilitäten führen. Die entfernte Nutzung einer unter Parallels Desktop betriebenen VM ist nur mit Mobilgeräten von Apple über das proprietäre Parallels Mobile Protokoll möglich.

Tabelle 4.8: Vergleich Lokale Desktop-Virtualisierung

| Produkt | VMware Workstation | Oracle VirtualBox | Parallels Desktop |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | – | ✓ | – |
| Lizenzkosten | pro Installation; Mengenrabatt ab 10 Lizenzen | –[87] | pro Installation; Mengenrabatt ab 5 Lizenzen |
| Einschränkungen | Max. 8 vCPU und 32 GB vRAM je VM | Max. 32 vCPU je VM. Unter OSS-Lizenz fehlen USB-2.0-Support, RDP und PXE boot | Max. 8 vCPU, 8 GB vRAM und 256 MB Grafik-RAM je VM. Unter MacOS X nur auf Intel VT-x, sonst auch auf AMD-V lauffähig. |
| **Grundfunktionen** | | | |
| Unterstützte Wirts-Plattformen<br>Windows XP/7/Linux/MacOS X | ✓/✓/✓/– | ✓/✓/✓/✓ | ✓/✓/✓/✓ |
| Unterstützte Gast-Plattformen<br>Windows XP/7/Linux/MacOS X | ✓/✓/✓/– | ✓/✓/✓/✓ | ✓/✓/✓/✓ |
| Standard-VM-Format | VMDK | VDI | HDD |
| Plattform-Konfiguration<br>(U)EFI/APIC/Chipsatz/Startreihenfolge | –/✓/✓/✓[88] | ✓/✓/✓/✓ | –/–/–/✓ |
| Logische Resourcenzuteilung<br>CPU/RAM/Grafik-RAM | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| Unterstützung USB-Geräte<br>USB-1.0/USB-2.0/USB-3.0 | ✓/✓/– | ✓/✓/– | ✓/✓/– |
| Medien-Unterstützung<br>Audio/2D-/3D-Beschl./Mehrere Monitore | ✓/✓/✓/✓ | ✓/✓/✓/✓ | ✓/✓/✓/✓ |
| Netz-Anbindung<br>NAT/Bridge/VM-Intern/Host-only | ✓/✓/–/✓ | ✓/✓/✓/✓ | ✓/✓/–/✓ |
| Transparente Paravirtualisierung | ✓ | ✓ | ✓ |
| Uhrzeit-Synchronisierung | ✓ | ✓ | ✓ |
| Netzwerk-Boot (PXE) | ✓ | ✓ | ✓ |
| **Desktop-Integration** | | | |
| Gasterweiterungen<br>Windows XP/7/Linux/MacOS X | ✓/✓/✓/– | ✓/✓/✓/✓ | ✓/✓/✓/✓ |
| Drag&Drop | ✓ | – | ✓[89] |

[87] Optional können Support-Lizenzen erworben werden.
[88] Automatisches Erkennen startfähiger Medien
[89] Nur zwischen MacOS X und Windows

| Produkt | VMware Workstation | Oracle VirtualBox | Parallels Desktop |
|---|---|---|---|
| Clipboard | ✓ | ✓ | ✓ |
| Nahtlose Integration[90] | ✓ | ✓ | ✓[91] |
| Gemeinsame Ordner | ✓ | ✓ | ✓ |
| Transparenter Fokuswechsel | ✓ | ✓ | ✓ |
| Treiberloses Drucken | ✓ | – | – |
| **Verwaltung** | | | |
| Im-/Export von OVF-Paketen | ✓ | ✓ | – |
| Erstellen von Zwischenständen | ✓ | ✓ | ✓ |
| Erstellen von Klonen | ✓ | ✓ | ✓ |
| Vorschlag Plattform-Konfiguration | ✓ | ✓ | ✓ |
| Monitoring | ✓ | ✓ | ✓ |
| Remote-Zugriff | ✓(VNC) | ✓(RDP) | –[92] |

**Empfehlungen:** Die VirtualBox von Oracle ist eine ausgereifte Open-Source-Software, die kaum Wünsche offen lässt und auf allen relevanten Plattformen mit allen betrachteten Gastsystemen gut zurecht kommt. Im Bedarfsfall kann professioneller Support von Oracle über entsprechende Lizenzen bezogen werden. Zwar gibt es mit dem fehlenden Drag&Drop zwischen Wirt und Gast und der PUEL-Lizenz für das Erweiterungspaket ein paar Wermutstropfen, doch überwiegt der positive Gesamteindruck bei Weitem. Diese Lösung sollte daher sowohl für die lokale Desktop-Virtualisierung als auch für die Plattformneutrale Anwendungs-Virtualisierung in Betracht gezogen werden.

Die VMware Workstation kann ebenfalls rundum überzeugen, die fehlende Unterstützung von MacOS X dürfte für die meisten Behörden nicht allzu schwer wiegen. Zwar handelt es sich um lizenzpflichtige proprietäre Software, doch unterstützt und propagiert VMware offene Standards, und mit der Lizenzierung erwirbt man zugleich professionellen Support. Auch diese Lösung ist daher einen näheren Blick wert.

Behörden mit der Notwendigkeit zur Unterstützung von MacOS X-Wirten oder -Gästen sollten die VirtualBox und Parallels Desktop gegenüberstellen. Letztere bietet eine gute Integration von Windows-Gästen in das Mac-Umfeld, unterstützt allerdings keinen der offenen Standards und zwingt zur Konvertierung von Fremdformaten in das nicht offen gelegte eigene HDD-Format. Bei einer späteren Verlagerung virtueller Maschinen, beispielsweise im Rahmen einer VDI-Lösung (siehe 4.2.5.1.3) in ein Rechenzentrum, sind Schwierigkeiten beim Betrieb solcher VMs wahrscheinlich. Daher muss genau geprüft werden, ob die lokalen Vorteile dieser Lösung den Nachteil der Inkompatibilität tatsächlich überwiegen.

Ohnehin sollte bei dieser Art von Virtualisierung bedacht werden, dass es sich meist nur um eine Übergangslösung handelt, bis entweder die virtualisierten Anwendungen auf die Wirts-Plattform portiert sind oder eine Virtual Desktop Infrastructure eingeführt ist, auf der die virtuellen Desktops dann dauerhaft betrieben werden. Größere Investitionen lohnen sich daher eher bei der Portierung oder der VDI-Einführung.

[90] Die in einer virtuellen Maschine gestartete Applikation fügt sich vollständig in den Wirts-Desktop ein (Startmenü, Task-Leiste, etc.).
[91] Unter MacOS X und Windows
[92] Fernsteuerung über Parallels Mobile mit iPhone/iPad/iPod touch möglich.

#### 4.2.5.7 Empfehlungen

Virtuelle Systeme bieten gegenüber physischen verschiedene Vorteile, die zu einfacherer Systemverwaltung, optimierter Systemsicherheit und besserer Hardwareauslastung führen. Die breite Verfügbarkeit von Prozessoren mit Virtualisierungsunterstützung und vielen Kernen bildet zusammen mit günstigem Arbeits- und Plattenspeicher eine tragfähige Grundlage für die Einführung oder den Ausbau virtueller Systeme. Behörden sollten sich dieser Entwicklung nicht verschließen, sondern sie aktiv aufnehmen.

Server-seitig bereitgestellte Dienste können ohne nennenswerte Auswirkungen auf die Anwender virtualisiert und darüber Erfahrungen im Migrationsprozess und der Verwaltung virtueller Systeme gesammelt werden. Ziele sollten eine bessere Hardware-Auslastung und eine höhere Verfügbarkeit der Dienste sein. Eine kostengünstige Form von Hochverfügbarkeitssystemen mit Virtualisierungstechnologie beschreibt beispielsweise (Hei11) auf Seite 108. Die eingesetzten Verwaltungswerkzeuge sollten die virtualisierten Dienste als OVF- oder OVA-Pakete bereitstellen können, um auf eine mögliche Verlagerung deren Ausführung in eines der DLZ-IT vorbereitet zu sein.

Die Virtualisierung von Desktops (VDI) verlangt zum einen eine leistungsfähige Virtualisierungs-Infrastruktur auf der Server-Seite mit entsprechender Erfahrung der Administratoren und andererseits die Abkehr der Anwender von der bisher gewohnten Arbeitsweise mit dem persönlichen Arbeitsplatzrechner (APC). Die Beschaffung von Thin Clients[93] ist eine sinnvolle Möglichkeit zur Unterstützung einer solchen Migration und verhindert zuverlässig lokale Sicherheitslücken und Datenhalden. Allerdings entstehen beträchtliche Hardwarekosten, und weitere Investitionen in das Behördennetz zur Bewältigung der höheren Bandbreiten sind wahrscheinlich. Eine schrittweise Migration ist daher anzuraten, die mit der Ersatzbeschaffung veralteter APCs synchronisiert werden sollte.

Die lokale Desktop-Virtualisierung ist für die überwiegende Mehrheit der Anwender keine sinnvolle Alternative zur VDI, da neben dem Wirts- auch alle Gastsysteme selbst gewartet werden müssen. Zudem sind für deren performanten Betrieb gute IT-Kenntnisse bei der Konfiguration der virtuellen Umgebung vonnöten. Diese Virtualisierungs-Alternative bleibt daher wenigen Abteilungen vorbehalten, die mit der Entwicklung oder dem Test von Systemen und Anwendungen betraut sind.

Die Windows-Sandboxes (siehe 4.2.5.5.3) sind ebenfalls keine sinnvolle Alternative zur VDI. Sie eliminieren lediglich die konzeptuellen Nachteile einiger Windows-Spezifika (Registry, DLL-Verwaltung), ermöglichen aber keine Plattform-Neutralität und sind mangels offener Standards allesamt proprietärer Natur.

#### 4.2.5.8 Terminaldienste

Die bereits in der letzten Fassung des Migrationsleitfadens betrachteten Terminal-Lösungen sind eine weitere Möglichkeit, den Betrieb vieler Desktop-Systeme zu vereinfachen. Wie bei der Desktop-Virtualisierung (VDI) wird die Ausführung von Anwendungen auf leistungsfähige Maschinen verschoben, deren Wartung dadurch zentralisiert und mit deutlich weniger Aufwand betrieben werden kann.

Allerdings ist eine einzelne Terminal-Sitzung im Gegensatz zur Desktop-Virtualisierung nicht vollständig autark und kann daher nicht losgelöst vom Wirtssystem und parallelen Terminal-Sitzungen verwaltet werden. Die Bedeutung von Terminal-Lösungen nimmt infolgedessen zugunsten der VDI ab; daher werden solche Lösungen nicht mehr in der bisherigen Detailtiefe betrachtet.

##### 4.2.5.8.1 Kriterien

Wer dennoch eine Migration zu Terminaldiensten in's Auge fassen möchte, sollte viele der für die verschiedenen Virtualisierungsarten genannten Kriterien berücksichtigen. Im größeren Maßstab eingesetzte Terminallösungen mit drei- oder vierstelligen Nutzerzahlen sollten die Terminalserver unter den gleichen Gesichtspunkten betreiben, wie sie für die Server-Virtualisierung genannt sind. Insbesondere eine effiziente Nutzung vorhandener Hardware, die automatische Lastverteilung und die Ausfallsicherheit

[93] Siehe beispielsweise die Migration Kopenhagener Krankenhäuser, http://heise.de/-1325878

sind zentrale Kriterien für den Erfolg solcher Lösungen. Daher sollten bei deren Auswahl die Kriterien der Server-Virtualisierung geprüft werden. Darüber hinaus sollten sie dahingehend untersucht werden,

- wie viele Terminals je Server-Instanz parallel genutzt werden können,
- welche Lizenzkosten pro Server-Instanz und pro Terminalsitzung entstehen,
- auf welchen Plattformen Terminalsitzungen möglich sind,
- ob offene Protokolle für den Zugriff auf Terminalsitzungen eingesetzt werden,
- ob alternative Sitzungs-Clients eingesetzt werden können und
- ob eine Ressourcen-Aufteilung oder -gewichtung zwischen Terminalsitzungen möglich ist.

Wie bei der (entfernten und lokalen) Desktop-Virtualisierung gilt es zudem, die Verwendung lokaler Geräte zu prüfen, vom Multi-Monitor-Betrieb über die Unterstützung von USB-Geräten und der Wiedergabe von Audio-Streams bis hin zu angeschlossenen Druckern.

#### 4.2.5.8.2 Produkte

Das Linux Terminal Server Project (LTSP)[94] ermöglicht den Einsatz von Linux als Terminalserver für Linux-Clients. LTSP ist in Schulen, Bildungseinrichtungen und Internet-Cafès verbreitet, da es server- und clientseitig wenig Hardware-Resourcen beansprucht und dadurch auch mit älteren, leistungsschwachen Rechnern genutzt werden kann. Allerdings stellt es relativ hohe Anforderungen an die Bandbreite des lokalen Netzwerks. LTSP steht unter der OSS-Lizenz GPL v2 zur Verfügung.

Der NX Server von NoMachine[95] kann wahlweise unter Linux oder Solaris betrieben werden und bietet eine gegenüber LTSP deutlich effizientere Nutzung der Netzwerk-Bandbreite. Die Anzahl möglicher paralleler Terminalsitzungen pro Server steigt dadurch deutlich. Andere Terminallösungen wie die Remote Desktop Services von Microsoft können so integriert werden, dass der NX Server als Mittler auftritt und die eigene Netzwerk-Effizienz vorteilhaft einbringt. Der Zugriff auf NX-Sessions ist auch mit Browsern unter verschiedenen Plattformen möglich, seine Stärken spielt der NX Server allerdings mit Linux-Clients aus. Der NX Server basiert zwar teilweise auf OSS, wird aber nur unter verschiedenen proprietären Lizenzen angeboten.

Die im letzten veröffentlichten Migrationsleitfaden aufgeführten Produkte von Microsoft (Windows Terminal Server) und Citrix (Presentation Server) weisen jeweils neue Namen auf (Remote Desktop Services bzw. Citrix XenApp). Für ihren Einsatz ist jeweils ein Windows Server 2008 R2 vonnöten, wobei die Citrix-Lösung den von Microsoft angebotenen Umfang an Funktionalität erweitert. Das Lizenzierungsmodell der Microsoft-Lösung ist komplex und verlangt neben Server-Lizenzen für alle verbundenen Clients ebenfalls Lizenzen. Diese Lizenzen müssen auch beim Einsatz der Citrix-Lösung erworben und um weitere Citrix-spezifische Lizenzen ergänzt werden. Das verwendete proprietäre Protokoll RDP liegt inzwischen in Version 7.0 vor, die neueren Eigenschaften können allerdings nur mit Windows 7 genutzt werden.

[94] http://de.wikipedia.org/wiki/Linux_Terminal_Server_Project
[95] http://www.nomachine.com/products.php

## 4.2.6 Client-Management

### 4.2.6.1 Einleitung

Als Client-Management wird die zentrale Verwaltung einzelner IT-Arbeitsplatzgeräte (Clients) in einem Behörden- oder Firmen-internen Netzwerk bezeichnet. Die Verwaltung umfasst die Erhebung und Vorhaltung von Geräte- und Anwendungsdaten sowie bestimmte zentralisierte Operationen auf den entfernten Geräten.

Mit zunehmender Größe einer Behörde steigt meist auch die Heterogenität der IT-Landschaft. Bezogen auf die Clients zeigt sich dies in

- verschiedenen Typen von Hardware (Notebooks, Desktops, Pads),
- verschiedenen Hardware-Herstellern und -Ausstattungen,
- verschiedenen Plattformen (Windows XP, Vista, 7, Linux, MacOS X) und
- verschiedenen fachlich notwendigen Anwendungen.

Permutationen über diese Arten von Heterogenität sind in beliebiger Anzahl anzutreffen und lassen vom Benutzer explizit dazu installierte Anwendungen noch außen vor. Die IT-Administratoren benötigen daher Werkzeuge, um die Verwaltung der Geräte beherrschen zu können.

Das Client-Management umfasst den kompletten Lebenszyklus von IT-Geräten. Es deckt die Installation, die Konfiguration und die Wartung sowie die Außerbetriebnahme von Betriebssystemen und Softwareprodukten (Anwendungen) ab. Im Rahmen des aktiven Lizenzmanagements werden Softwarepakete, die auf einem Client nicht mehr benötigt werden, deinstalliert und dem Softwarepool wieder zur Verfügung gestellt. Seit Kurzem gehört auch die Bereitstellung und Verwaltung von virtuellen Maschinen (Provisionierung) zu den Aufgaben des Client-Managements.

Die Verteilung von Software setzt auf Softwarepaketen auf. Diese werden häufig bereits vom Lieferanten der Software verteilfähig bereitgestellt. Ist dieses nicht der Fall, müssen die Pakete vor der Verteilung noch mit geeigneten Werkzeugen erstellt werden.

Das Client-Management ist grundsätzlich für alle Desktop-Plattformen von Bedeutung. Im Behördenbetrieb kann dies allerdings auf die Windows-Plattformen und Linux-Derivate eingeschränkt werden, da MacOS X-basierte Geräte hier noch kaum Verbreitung gefunden haben.

Das Management von Serversystemen und Server-basierten Terminal-Serversystemen wird in diesem Abschnitt nicht betrachtet. Terminal-Serversysteme bringen von Haus aus eigene Managementlösungen mit, die im Zusammenspiel mit den Werkzeugen des Client-Managements verwendet werden können.

### 4.2.6.2 Kriterienkatalog

Das wichtigste Ziel des Client-Managements ist es, standardisierte Services wesentlich schneller und verlässlicher zu erbringen, als das mit einer manuellen Methode möglich wäre. Dazu müssen die relevanten Informationen zentral zusammengeführt werden, um darauf aufbauend Teilinformationen gezielt bereitstellen und die Installation und Wartung von Software soweit wie möglich automatisieren zu können.

Insbesondere bei der Planung von Anwendungsmigrationen ist es erforderlich, präzise Informationen über die Client-Plattformen zu haben. Ein Betreiber von Client-Systemen muss daher wissen, welche Clients in welcher Ausstattung sich in seinem Netzwerk befinden. Die **Inventarisierung von Hardware** ist daher eine grundlegende Funktionalität des Client-Managements. Die Inventarfunktion des Client-Managements umfasst idealerweise neben den eigentlichen Clients auch die unterstützenden Infrastrukturkomponenten im Netzwerk sowie Drucker.

Im Umgang mit Lizenzkosten-pflichtiger Software ist es notwendig, über ein **Software-Inventar** stets exakte Zahlen über aktive Installationen abrufen und darüber ein verlässliches **Lizenzmanagement** betreiben zu können. Betriebssysteme und benötigte Software müssen **verteilt** und auf dem aktuellen

Stand gehalten werden können (**Patch-Management**). Zudem sollten IT-Administratoren das Verhalten der Clients im Netz beeinflussen und ggf. notwendige lokale Änderungen von ihrem Arbeitsplatz aus durchführen (**Remote-Administration**) können. Der **Helpdesk** wiederum sollte die Anwender durch exakte Informationen über den aktuellen Zustand deren jeweiligen Arbeitsgeräts besser unterstützen können.

#### 4.2.6.3 Methodik

In einer **Ist-Analyse** sollte eine ggf. vorhandene Client-Management-Lösung dahingehend untersucht werden, welche Informationen sie in welcher Detailtiefe vorhält, wo sie diese Informationen ablegt und ob die Ablage für Datenexporte oder -extraktionen geeignete Möglichkeiten bietet. Insbesondere sollte geprüft werden, ob die Daten in einem Verzeichnisdienst (siehe 4.2.3) abgelegt sind, auf den per LDAP zugegriffen werden kann.

Ebenfalls festgestellt werden sollte die Art der Informationsbeschaffung und die ggf. genutzten Schnittstellen. Daraus sollte hervorgehen, ob auf den lokalen Arbeitsplatzgeräten Hilfssoftware zur aktiven Übertragung von Zustandsinformationen an die Client-Management-Lösung installiert ist oder diese Informationen beispielsweise per WMI oder WBEM (siehe 4.2.2.1.3) zentral abgefragt werden.

Von den IT-Administratoren sollte erfragt werden, welche der im Kriterienkatalog genannten Funktionalitäten derzeit vorhanden sind, welche davon genutzt werden und welche fehlen. Auch ohne IT-gestütztes Client-Management sollten diese darüber Auskunft geben können, welcher Grad an Heterogenität hinsichtlich der Geräte, Betriebssysteme und Standard-Anwendungen besteht. Die Erkenntnisse zu den letzten beiden Themen sollten erkennen lassen, ob es sich in der Behörde im Wesentlichen um Produkte desselben Herstellers, namentlich um Microsoft-Produkte handelt.

Die anschließende **Soll-Konzeption** sollte die derzeit genutzten Informationen und Funktionalitäten als Basis-Funktionalität voraussetzen und die als fehlend eingestuften hoch priorisieren. Die künftige Lösung sollte in der Lage sein, den ggf. vorhandenen Informationsbestand unmittelbar oder per Extraktion und Import weiter zu nutzen. Die Zielsetzung sollte die vollständige Unterstützung der im Kriterienkatalog genannten Aspekte sein, möglichst flankiert von Schnittstellen zu Werkzeugen für das Konfigurationsmanagement. Die IT-Administration sollte durch die Einführung der künftigen Client-Management-Lösung von bisher notwendigen Routinearbeiten entlastet werden. Auf eine möglichst stark automatisierte Softwareverteilung und -aktualisierung sollte daher ebenso Wert gelegt werden wie auf eine einfache Form der Informationsgewinnung.

#### 4.2.6.4 Betrachtete Alternativen

Am Markt gibt es sowohl für Linux als auch für Windows eine Reihe von Client-Management-Lösungen. Diese werden in den nachfolgenden Abschnitten detaillierter betrachtet. In beiden Bereichen stehen sowohl Anwendungen zur Verfügung, die ohne weitere Investitionen in Lizenzen und Wartung genutzt werden können, als auch kostenpflichtige Produkte. Dabei gehen die kostenpflichtigen Produkte im Funktionsumfang und Komfort über die Möglichkeiten der kostenfrei verfügbaren Werkzeuge hinaus und können so je nach Einsatzgebiet die Zusatzkosten rechtfertigen. Lösungen zur Verwaltung heterogener Umgebungen sind in 4.2.6.4.3 dargestellt. In Abschnitt 4.2.6.4.3 werden ergänzend Lösungen betrachtet, die nur Inventory-Funktionen haben.

Ein wesentlicher Unterschied zwischen Windows und Linux besteht in der Art der Konfiguration von Client-Systemen. Unter Linux sind dafür in der Regel Konfigurationsskripte zuständig, während unter Windows eine Gruppenrichtlinie gesetzt wird, die dann mithilfe des AD über die Domäne verteilt wird. Client-Management-Werkzeuge setzen hierauf auf und entlasten den Administrator in vielen Bereichen davon, sich mit den technischen Details des jeweiligen Systems auseinandersetzen zu müssen. Allerdings können die meisten Funktionen der Client-Management-Werkzeuge mit entsprechendem Wissen und Aufwand auch mit Bordmitteln der jeweiligen Betriebssysteme umgesetzt werden.

Die in 4.2.2 genannten kommerziellen Systemüberwachungs-Lösungen bieten auch Module zum Client-Management an. Sofern erstere bereits im Einsatz sind, ist eine Ergänzung um Module für das Client-Management sinnvoll und vergleichsweise günstig. Andernfalls ist eine Beschaffung dieser Produkte für die Aufgaben des Client-Managements aufgrund der Kosten und Komplexität eher untypisch.

#### 4.2.6.4.1 Linux-basiertes Client-Management

Die Softwareverteilung des Client-Managements zur Auslieferung und Aktualisierung von Softwarekomponenten stützt sich unter Linux auf Softwarepakete und eine entsprechende Paketverwaltung. Zwischen den einzelnen Distributionen gibt es unterschiedliche Standards für die Erstellung und Auslieferung der Pakete. Verbreitet sind Pakete im Red Hat- (RPM) und im Debian-Format (DEB), die über Hilfsmittel[96] in das jeweils andere Format gewandelt werden können.

Die Distributionen Suse Linux Enterprise Server (SLES), CentOS und Red Hat Enterprise Linux (RHEL) verwenden beispielsweise das RPM-Format und darauf basierende Werkzeuge, während Debian, UCS und Ubuntu das DEB-Format und entsprechende Werkzeuge einsetzen. Zwar sind die Paketmanager auf das jeweilige Format abgestimmt und dadurch unterschiedlicher Natur, in ihrer jeweiligen Funktionalität allerdings sehr ähnlich. Alle genannten Distributionen bieten automatische Updates für das Betriebssystem und alle über den Paketmanager installierten Anwendungen. Die Bezugsquellen für Softwarepakete können beliebig angepasst und beispielsweise auf Behörden-eigene Quellen für Fachverfahren ausgedehnt werden. Auch können die Aktualisierungen beispielsweise auf Versionen mit Langzeitunterstützung eingeschränkt werden.

Neben der Paketverwaltung hat sich unter Linux ein einheitlicher Standard für das Verteilen von Dateien und Programmen im lokalen Dateisystem etabliert (Linux Standard Base – File Hierarchy Standard). Dieser Standard deckt auch die Regeln für die Installation von Drittsoftware wie Oracle-Datenbanken oder SAP-Systemen ab.

Alle RPM- und DEB-basierten Distributionen können mit dem freien Werkzeug **Fully Automatic Installation (FAI)**[97] automatisch installiert werden. Hierzu konfiguriert der Administrator das Profil der gewünschten Desktop- oder auch Serverinstallation. Von der Partitionstabelle über die Auswahl der zu installierenden Softwarepakete bis hin zu den lokalen Konfigurationsdateien ist alles abgedeckt, so dass eine automatische Installation ohne Eingriff des Administrators jederzeit möglich ist.

Einige Hersteller von Linux-Distributionen bieten kostenlose Update Services für ihre Distributionen an. Eine besonders komfortable Lösung ist **Spacewalk**[98] von Red Hat. Damit werden lokale Clients direkt mit dem Red Hat-eigenen Software-Distributionsmechanismus synchronisiert. Der aktuelle Patch-Stand auf verschiedenen Systemen ist dabei jederzeit einsehbar. Außerdem bietet Red Hat seinen Abonnement-Kunden Einblick in die Klassifizierung der Updates, so dass über diese Klassifizierung und den zugehörigen Verweis auf ein aktuelles Security-Advisory schnell die Relevanz des jeweiligen Patches eingeschätzt werden kann. Problematisch ist die Installation von Software-Paketen, die nicht vom Hersteller geliefert werden. Hier ist es zumindest bei der Red Hat-Lösung Spacewalk notwendig, ein eigenes Verzeichnis der zu installierenden Software anzulegen und einen Management-Server lokal zu betreiben.

Canonical bietet für Ubuntu das Werkzeug **Landscape**[99] an, welches ähnliche Eigenschaften wie Spacewalk aufweist und neben dem Client-Management auch für die Systemüberwachung genutzt werden kann.

Eine umfassende Systemkonfiguration wird durch Tools wie **CFengine**[100] realisiert. Die textbasierten Konfigurationsdateien von Linux werden aufgespalten und sind umfassend automatisierbar. Einzelne

[96] Beispielsweise über das Werkzeug *alien*
[97] http://fai-project.org/
[98] http://spacewalk.redhat.com/
[99] https://landscape.canonical.com/
[100] http://www.cfengine.org/

Profile regeln, welcher Rechner welche Konfigurationsparameter bekommt (CFengine wird z.B. als Teil von FAI eingesetzt).

#### 4.2.6.4.2 Windows-basiertes Client-Management

**Windows Deployment Services (WDS)** sind die Standardmethode von Microsoft zum Massenrollout von Clients und Software auf Windows-Plattformen. WDS bieten die Möglichkeit, aus den Standard-Microsoft-Betriebssystemen vielfach verteilbare Images zu erstellen, die dann zum standardisierten Aufsetzen automatisiert verwendet werden können. Viele Einstellungen, die nicht über eine Gruppenrichtlinie veränderbar sind, können durch die WDS eingestellt werden. Mit WDS können außer Clients auch Server bereitgestellt werden.

Zur Wartung von Windows-Clients gibt es mehrere Optionen. Microsoft bietet zum einen den kostenlosen **Windows Server Update Service (WSUS)**, der die hauseigenen Komponenten auf dem aktuellen Stand halten kann. Zum anderen ist der kostenpflichtige **System Center Configuration Manager (SCCM)** erhältlich, mit dem beliebige Software ausgerollt werden kann.

WSUS ist hochgradig automatisiert. Wie unter Linux werden alle verfügbaren Patches automatisch klassifiziert und auf Wunsch auch automatisch installiert. SCCM bietet weitergehende Möglichkeiten zur Auslieferung von Software und kann beispielsweise die Arbeitslast auf mehrere Server verteilen und koordiniert ablaufen lassen. Prinzipiell können über die Ausführung von entsprechenden Skripten und Programmen mit SCCM beliebige individuell benötigte Abläufe durchgeführt werden. SCCM verfügt über umfangreiche Inventarisierungsfunktionen.

**Opsi (open pc server integration)**[101] ist eine im Kern freie Lösung zum Management von Windows Clients, die auf Linux Servern läuft. Sie deckt die Funktionen Betriebssystem- und Softwareverteilung, Patchmanagement und Inventarisierung von Hardware und Software ab. Die Integration in die Windows-Mechanismen des Active Directory ist bei dieser Lösung naturgemäß geringer als bei den Microsoft-Produkten.

#### 4.2.6.4.3 Heterogenes Client-Management

Zum Management von heterogenen Client-Umgebungen gibt es am Markt mehrere kommerzielle Lösungen von Drittanbietern, die sich darauf spezialisiert haben, das Client-Management für mehrere Betriebssystem-Plattformen mit einem zentralen Werkzeug durchzuführen. Die nachfolgend vorgestellten Produkte gehen alle über das Kerngebiet des Client-Managements hinaus.

Die **Altiris-Werkzeuge** der Firma Symantec unterstützen Clients unter Windows, Linux und Mac OS. Symantec erweitert mittlerweile deutlich die in der „Altiris Client-Management Suite“ verfügbaren Grundfunktionen des Client-Managements und bietet ein breites Portfolio zum Thema Service-Management an. Der Altiris-Funktionsumfang reicht dabei von der Inventarisierung und automatischen Suche von Hard- und Softwarekomponenten über das Imaging von Client-Systemen bis hin zur Fernunterstützung von Anwendern.

Die **Empirum-Software** der Firma Matrix42 zum Client-Management ist ebenfalls in ein umfangreiches Portfolio eingebettet. Sie unterstützt das Client-Management unter Windows und Linux. Neben dem üblichen Funktionsumfang im Bereich Softwareverteilung und Inventarisierung hat Matrix42 einen Schwerpunkt in der integrierten Verwaltung und Abwicklung von Hardware- und Softwareanforderungen seitens der Endanwender.

**ZENworks** von Novell unterstützt die Kernfunktionen Asset Management, Software und Patch Management des Client-Managements auf den Plattformen Windows und Linux. Weitergehende Funktionen betreffen die Bereiche Sicherheitsmanagement auf Clients und Configuration Management.

[101] http://www.opsi.org

#### 4.2.6.4.4 Inventory

Inventory-Systeme katalogisieren die eingesetzte Hardware, Firmwarestände und Software. Die Herausforderung dabei ist, jeweils den für die Aufgabenstellung angemessenen Detaillierungsgrad festzulegen.

In der Klasse der reinen Inventory-Systeme gibt es verglichen mit den Management-Systemen einen deutlichen höheren Anteil von Lösungen, die Plattform-übergreifend arbeiten. Beispielsweise bietet Symantec als Teil der „Altiris Client Management Suite“ eine Lösung für das Inventory an. Im Open-Source-Bereich gibt es mit **OCS Inventory**[102] und **FusionInventory**[103] leistungsfähige Lösungen, die neben Windows auch ein breites Spektrum an Linux- und Unix-Clients unterstützen.

Inventory-Systeme haben verschiedene Möglichkeiten, die Erkennung von Hard- und Softwarekomponenten (Discovery Prozess) zu betreiben. In der Regel werden die in 4.2.2.1.3 dargestellten Schnittstellen genutzt, insbesondere die universellen Schnittstellen SNMP, WBEM und WMI. Drucker und Netzwerkkomponenten werden in der Regel über SNMP abgefragt. Sollen auf den Clients keine Agenten installiert werden, so wird neben SNMP das wesentlich mächtigere WMI genutzt, über das Windows-Clients u.a. zu installierter Software abgefragt werden können. Linux-Clients wiederum können mittels lokal installierter WBEM-Daemonen wie dem **small footprint CIM broker (SFCB)** zu diversen Hard- und Software-Aspekten befragt werden. Für MacOS X existiert mit dem **Apple Remote Desktop management tool** eine ebenfalls WBEM-basierte Möglichkeit zur Abfrage von Systeminformationen.

### 4.2.6.5 Empfehlungen

Der Einsatz einer Lösung zur Inventarisierung von Hardware und Software ist heute die Mindestanforderung an ein Client-Management-System. Handelt es sich um eine statische Umgebung oder eine Landschaft, in der die Anwender sich selbst um die Pflege ihrer Clients kümmern, kann auf die aktive Verwaltung von Clients mit Client-Management-Systemen verzichtet werden. In diesen Fällen ist der Einsatz eines einfachen Inventory-Werkzeuges ausreichend.

Im Regelfall eines aktiv verwalteten Clients ist der Einsatz eines Client-Managementwerkzeuges sinnvoll, mit dem manueller Administrationsaufwand und Vor-Ort-Support eingespart werden kann. Hierbei muss darauf geachtet werden, dass die Softwarelieferanten verteilfähige Pakete liefern oder zumindest Unterstützung bei der Erstellung dieser Pakete für alle relevanten Betriebssystem-Plattformen anbieten.

In beiden Fällen sollte darauf geachtet werden, dass der universelle und freie Standard WBEM zur Gewinnung von Systeminformationen unterstützt wird. Ebenfalls beachtet werden sollte, dass die Lösung die Ablage der Client-Management-Daten in einem LDAP-fähigen Verzeichnisdienst unterstützt.

[102] http://www.ocsinventory-ng.org/
[103] http://fusioninventory.org/

## 4.3 Desktop und unterstützende Systeme

### 4.3.1 Einleitung

Dieses Kapitel befasst sich mit IT-Lösungen, die viele Beschäftigte von Bundesbehörden regelmäßig an ihrem Arbeitsplatz einsetzen und die für ihre Tätigkeit notwendig sind. Im Gegensatz zu Fachanwendungen sind diese Lösungen für allgemeine Aufgaben ohne Fachbezug verwendbar. Die einzelnen Themen sind in Abbildung 4.3 dargestellt.

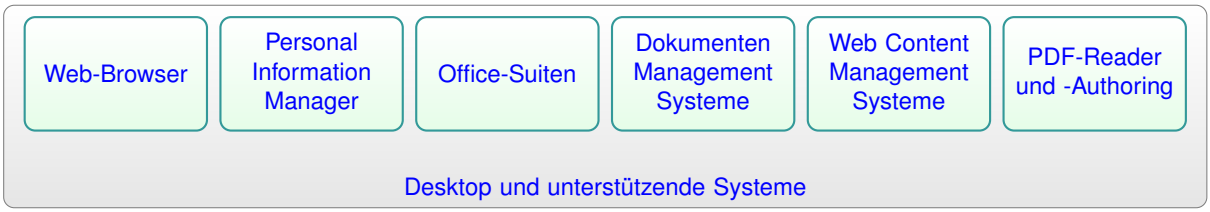


**Abbildung 4.3:** Migrationsthemen

In der letzten veröffentlichten Fassung des Migrationsleitfadens wurden einige dieser Themen im Modul III: Anwendungen diskutiert. Von den dortigen Themen wird „Office / Desktop“ nun unter Office-Suiten beleuchtet, „Teaming-/Workgroup Software“ wird durch die Themen Dokumenten Management Systeme und Web Content Management Systeme ersetzt. Die Themen „Messaging und Groupware“ sowie „Terminal-Dienste und Client-Konzepte“ werden im Kapitel zur Infrastruktur in den Abschnitten Groupware und Virtualisierung und Terminaldienste diskutiert.

Neu hinzugekommen sind die Themen Personal Information Manager, Web-Browser und PDF-Reader und -Authoring. Das Thema „Backend-Integration“ ist entfallen.

## 4.3.2 Web-Browser

### 4.3.2.1 Einleitung

Der Web-Browser oder kurz der Browser ist für Viele bereits das meist verwendete lokale Werkzeug im Arbeitsalltag, da Anwendungen immer häufiger ihre Benutzeroberflächen über den Browser zur Verfügung stellen. Diese Entwicklung wird durch die zunehmende Verbreitung der Technologie Asynchronous JavaScript and XML (AJAX) und den darauf basierenden Rich-Internet-Applications (RIAs) begünstigt, die eine Realisierung von Rich-Client-Funktionalität im Browser ermöglichen. Der Web-Browser ist daher ein zentrales Thema bei jeder Migrationsplanung.

### 4.3.2.2 Kriterienkatalog

Von heutigen Browsern wird erwartet, dass sie bereits von Haus aus ein breites Spektrum an Funktionalitäten abdecken. Zur Pflicht gehört die **Unterstützung verbreiteter Protokolle**, die die Basis der Kommunikation in Netzwerken darstellen und daher obligatorisch sind. Bei deren Auswahl ist zu beachten, welche Protokolle gegenwärtig und in absehbarer Zeit zur Datenübertragung in Netzwerken verwendet werden.

Der Aspekt der **Sprachenunterstützung** analysiert, welche Programmier- bzw. Auszeichnungssprachen gegenwärtig am häufigsten verwendet werden, um Informationen im Internet bzw. Intranet darzustellen. Damit wird erreicht, dass der Browser einen Großteil der verfügbaren Webseiten darstellen (rendern) kann.

In den angesprochenen Auszeichnungs- bzw. Programmiersprachen sind viele Medientypen eingebettet. Folglich wird in dem Bewertungskriterium **Medientypenunterstützung** analysiert, welche der am häufigsten verwendeten Formate unterstützt werden. Dies trägt ebenfalls zu einer problemlosen Ausgabe von Web-Inhalten bei.

Die **Erweiterbarkeit** eines Browsers zur Darstellung weiterer Medientypen, zur Anpassung des Browser-Verhaltens oder dessen Aussehens gilt es ebenso zu untersuchen wie dessen Verfügbarkeit auf der gewünschten **Plattform**.

Die zunehmenden Anforderungen an Browser, unterschiedlichste Standards und Protokolle zu unterstützen, und die Notwendigkeit, viele Medienformate darzustellen, führt zu einer breiten Angriffsfläche für Hacker. Demzufolge wird durch das Bewertungskriterium **Sicherheitsmaßnahmen** analysiert, welche Schwachstellen auftreten und in welcher Zeit sie bereinigt werden. Zu beachten ist hier, dass Browser zur Darstellung proprietärer Medientypen Erweiterungen verwenden, die ebenfalls Angriffsflächen bieten. Diese sind separat auf Schwachstellen und deren Behebung zu analysieren.

### 4.3.2.3 Methodik

Der erste Schritt bei der Migrationsplanung von Web-Browsern ist die Analyse, welche **Auszeichnungssprachen**, **Protokolle** und **Medientypen** die aktuell eingesetzten Browser unterstützten. Dazu eignet sich neben Herstellerspezifikationen vor allem Testsoftware[104]. Sind die am häufigsten eingesetzten Browser nicht bekannt, eignen sich geltenede Regelungen (z.B. Verwendung von Firefox 3.x vorgeschrieben) oder die Analyse von Web-Server-Log-Files (HTTP User-Agent-Header) als Mittel zur Bestimmung der Häufigkeitsverteilung.

Das BSI ist die erste Anlaufstelle für die Beurteilung der **Sicherheit** von Browsern und hat hierzu verschiedene Dokumente veröffentlicht[105]. Für die Bestimmung der Wirksamkeit vorhandener **Sicherheitsmaßnahmen** eignet sich wiederum die Analyse von Datenbanken[106], die CVE von Browsern dokumen-

[104] http://www.webstandards.org/action/acid3/, http://w3c-test.org/html/, http://www.w3.org/MarkUp/Test/HTML401/current/tests/index.html oder http://samples.msdn.microsoft.com/ietestcenter/#html5 abgerufen: 31.03.2011

[105] siehe u.a. https://www.bsi.bund.de/DE/Themen/InternetSicherheit/WWW/WebClient/webclient_node.html

[106] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4643 oder http://www.cvedetails.com/, abgerufen: 31.03.2011

tieren. Derartige Archive sind i.d.R. äußerst detailliert und bieten somit einen sehr guten Überblick, welche Sicherheitsprobleme die verwendete Browser-Version hat. Generell wird bei der Einschätzung von Sicherheitsaspekten eine enge Zusammenarbeit mit der dafür zuständigen Person empfohlen, um eine ausreichend detaillierte Betrachtung zu gewährleisten.

Die Soll-Konzeption für die **zu unterstützenden Protokolle**, **Sprachen** und **Medientypen** ist teilweise durch deren Ist-Analyse gegeben, denn eine Abwärtskompatibilität bzgl. der Webstandards ist auf Grund der Heterogenität im Internet stets notwendig. Zusätzlich dazu ist zu prüfen, ob neuere Versionen der Standards existieren. Dadurch wird auch eine künftige Nutzbarkeit des Browsers gewährleistet. Die aktuellen Versionen der Protokolle, Sprachen und Medientypen lassen sich über Standardisierungsgremien[107] feststellen. Bei dieser Betrachtung fallen allerdings proprietäre Medientypen durch das Raster. Die Notwendigkeit deren Unterstützung hängt grundsätzlich von der Aufgabenstellung der jeweiligen Behörde ab, ist also domänenspezifisch. Allerdings haben sich im Laufe der Zeit einige De-facto-Standards gebildet, die ebenfalls zu berücksichtigen sind, weil sonst viele Webseiten nicht passend darstellbar wären. Zur Ermittlung der hier in Frage kommenden Formate sind adäquate Statistiken[108] zu Rate zu ziehen. In einem so dynamischen Umfeld wie dem Internet sollten außerdem auch kommende Standards beachtet werden, die kurz vor der Verabschiedung stehen, um nicht bald schon wieder Migrationsentscheidungen zu Web-Browsern treffen zu müssen.

Browser müssen mit den verschiedensten Medientypen zurechtkommen und sollten ihr Verhalten und Aussehen weitmöglichst an die Anforderungen der jeweiligen Benutzer anpassen lassen. Die Grundausstattung eines Browsers sollte sich daher möglichst einfach in die gewünschte Richtung erweitern lassen. Bei der **Erweiterbarkeit** wird zwischen Plug-Ins und Extensions unterschieden. Erstere sind für das Darstellen einzelner Medientypen zuständig und liegen wegen des schnellen Zugriffs auf Betriebssystemressourcen in Binärformaten vor, während Zweitere regelmäßig in Textform (JavaScript, CSS, HTML, XML) ausgeliefert werden. Plug-Ins sind hinsichtlich der Sicherheit des Browsers kritischer zu betrachten als Extensions, da hier keine unmittelbare Inspektion des zu Grunde liegenden Codes möglich ist und sie naturgemäß Zugriff auf Systemressourcen beanspruchen. Das Einschleusen von Schadsoftware ist daher über Browser-Plug-Ins leicht möglich. Für eine gute Erweiterbarkeit ist es notwendig, dass die Spezifikation zum Erstellen einer Browser-Erweiterung offenliegt, sie verständlich und einfach umsetzbar ist und es geeignete Sicherheitsmechanismen gibt, die das sichere Beziehen solcher Erweiterungen regeln, unerlaubte Zugriffe derselben auf andere als die vorgesehenen Browserbereiche wirksam unterbinden und den Absturz des Browsers beim Ableben einer Erweiterung verhindern.

Die Ausarbeitung des Soll-Zustands weiterer **Sicherheitsmaßnahmen** ist problematisch, da der Prozess des Schließens einer Sicherheitslücke i.d.R. erst nach deren öffentlichem Bekanntwerden in Gang gesetzt wird. Folglich sollte zunächst geklärt werden, ob die bekannten Sicherheitslücken der aktuell verwendeten Browser geschlossen sind. Dies erschließt sich über die Analyse der Status der CVE in den o.g. Datenbanken. Anschließend ist zu analysieren, welche gängigen Probleme bei Web-Anwendungen existieren, denn häufig sind sie und nicht der Browser Ausgangspunkt von Angriffen. Zur Feststellung derartiger Angriffsvektoren ist eine Analyse adäquater Studien optimal[109]. Bietet ein Browser dagegen wirksame Sicherheitsmaßnahmen, ist dies ein Vorteil, der in die Bewertung einfließen sollte.

Schließlich gilt es, die Anforderungen an den **Ressourcenverbrauch** und die Reaktionsgeschwindigkeit zu bestimmen. Heutige Browser sollten auf überladene Oberflächen verzichten und sich auf eine möglichst schnelle Darstellung der Webseiten-Inhalte konzentrieren. Ein zügiger Start des Browsers sollte ebenso selbstverständlich sein wie die schnelle Darstellung komplexer Webseiten und das flotte Übersetzen aktiver Inhalte wie JavaScript. Da sich der Ressourcenverbrauch eines Browsers hauptsächlich über die Anzahl geladener Webseiten und die zu rendernden Inhalte bestimmt, ist eine generelle

[107] Die wichtigsten Standardisierungsgremien für das Internet sind IETF, W3C und OASIS

[108] http://www.riastats.com/, http://www.adobe.com/products/player_census/shockwaveplayer/ oder http://httparchive.org/interesting.php abgerufen: 18.03.2011

[109] http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project oder http://www.sans.org/top25-software-errors/, abgerufen: 16.03.2011

Aussage zum maximalen Hauptspeicherbedarf nicht sinnvoll. Allerdings sollte mit dem Schließen einer Webseite der dafür benötigte Ressourcenbedarf im Wesentlichen wieder freigegeben werden.

Neben der Bestimmung des Soll-Zustands müssen vorhandene **Abhängigkeiten** und deren Auswirkungen auf eine Migration des Browsers beleuchtet werden. Insbesondere gilt es zu prüfen, ob bestimmte Browser-Plug-Ins für die Nutzung Web-basierter Fachanwendungen notwendig sind. Der häufigste Fall hierbei ist der Einsatz von ActiveX-Controls, die lediglich mit dem Microsoft Internet Explorer genutzt werden können. Sind solche Fachverfahren vorhanden, ist das Verlassen der Browser-Produktlinie nicht möglich, sondern lediglich eine fortführende Migration innerhalb derselben. Allerdings sollte für solche Fachverfahren untersucht werden, ob der Einsatz dieser Technologie tatsächlich *notwendig* ist oder lediglich eine Aussehens- oder Verhaltensänderung darstellt, die auch Skript-basiert als *Extension* umgesetzt werden könnte. Zudem sind im kommenden Standard HTML5 viele technische Neuerungen enthalten, die evtl. den Einsatz solcher proprietärer Erweiterungen ablösen können.

Nach der Durchführung der soeben geschilderten Schritte sind der aktuelle Stand der Browser-Landschaft und die Anforderungen an das Migrationsziel definiert. Eine **Vorauswahl** ist notwendig, denn alle Browser in den Testprozess miteinzubeziehen wäre zu zeit- und kostenaufwändig. Am einfachsten ist es hier, Browser-Nutzungsstatistiken aus dem Internet zu Rate zu ziehen, denn daran zeigt sich zumindest ein gewisser Trend, welche Anbieter die größten Marktanteile haben. Darauf basierend sind die aktuellen Versionen der Browser festzustellen. Zu beachten bei der Vorauswahl ist, dass unter bestimmten Umständen auch das Miteinbeziehen des aktuell verwendeten Browsers sinnvoll sein kann. Dazu ist vor allem die Untersuchung der Sicherheitsmaßnahmen bei der Ist-Analyse relevant. Schließt der aktuelle Browser hier gut ab, darf er durchaus berücksichtigt werden.

Auf die Vorauswahl folgt die tatsächliche **Bewertung**. Ob die derzeit relevanten **Protokolle, Programmier-/Auszeichnungssprachen** und **Medientypen** unterstützt werden, lässt sich anhand der Herstellerspezifikationen und mittels Testprogrammen verifizieren. Dabei ist zu beachten, dass diverse Medientypen nicht nativ vom Browser, sondern durch Erweiterungen dargestellt werden. Folglich ist auf der Webseite des Formatherstellers oder auf vertrauenswürdigen Sammelseiten für Erweiterungen zu überprüfen, ob eine passende Erweiterung existiert. Die Bewertung der Wirksamkeit von **Sicherheitsmaßnahmen** kann oberflächlich durch Onlinetests vertrauenswürdiger Seiten durchgeführt werden[110]. Ist zu erwarten, dass kritische Unternehmensdaten intensiv mit dem Browser bearbeitet werden, sollten Testberichte und Studien renommierter Testinstitute zu Rate gezogen werden, bevor eine Entscheidung getroffen wird.

Neben den soeben geschilderten allgemeinen Anforderungen sind weitere **domänenspezifische Bewertungskriterien** zu berücksichtigen. Dazu zählt unter anderem die Unterstützung nicht standardisierter Medientypen. Das Video-Containerformat DivX ist beispielsweise für Behörden eher weniger relevant, während eine gelungene Darstellung älterer Office-Dateien (z.B. DOC oder ODT 1.0) im Browser von Interesse sein kann.

Ebenfalls domänenspezifisch von Interesse sind beispielsweise integrierte Web-Seiten-Debugger oder eine Web-Seiten-Quelltextanzeige. Ein Browser, der in diesem Gebiet viele Optionen anbietet, ist für Behördenmitarbeiter mit starker technischer Ausrichtung eine sinnvolle Wahl, während die übrigen Mitarbeiter der Behörde diese Möglichkeiten des Browsers kaum oder gar nicht nutzen dürften.

Weitere kritische, aber stark domänenspezifische Anforderungen sind die Komfortfunktionen und die Benutzeroberfläche des Browsers. Weist die Analyse der Browser-Landschaft z.B. darauf hin, dass primär stark veraltete Browser-Versionen verwendet werden, gilt es, bei der Migrationsentscheidung die Innovationsaffinität der Anwender zu berücksichtigen. Ist zu erwarten, dass diese privat eher mit moderneren Browsern surfen, sollten z.B. Tabbed-Browsing oder ausgeblendete Menüleisten als Soll-Kriterium beachtet werden.

[110] http://www.heise.de/security/dienste/Browsercheck-2107.html, abgerufen: 31.03.2011

#### 4.3.2.4 Betrachtete Alternativen

Der Browser-Markt ist in ständiger Bewegung. Neben den etablierten Produkten Microsoft Internet Explorer und Mozilla Firefox gewinnen Alternativen wie Apple Safari, Google Chrome/Chromium oder Opera beständig an Boden. Verlässliche Aussagen über die tatsächliche Aufteilung des Browsermarkts gibt es allerdings nicht. Es liegen lediglich Annäherungen verschiedener Quellen vor, die die Häufigkeitsverteilung über Log-Einträge oder nicht repräsentative Online-Umfragen zu ermitteln versuchen[111] (Bec05). Die Vorauswahl der Browser-Alternativen basiert daher ebenfalls auf Schätzungen. Es werden folgende Produkte betrachtet:

- **Mozilla Firefox:** Stellt die gängigste Open-Source Variante dar und ist auch in Behörden weit verbreitet.
- **Microsoft Internet Explorer:** Teilt sich mit Firefox zusammen die Marktführerschaft in Deutschland und ist als Bestandteil von Microsoft Windows-Installationen in Behörden ebenfalls weit verbreitet.
- **Safari:** Ist der Standard-Browser auf Apple-Systemen[112], welche in Behörden allerdings derzeit kaum vorhanden sind. Der Browser existiert allerdings auch für Windows-Betriebssystem und ist deshalb durchaus relevant.

Anzunehmen ist, dass künftig auch Google Chrome / Chromium eine starke Rolle spielen wird, zumal mit der Google Inc. ein finanzielles Schwergewicht dessen Entwicklung vorantreibt.

#### 4.3.2.5 Bewertung

Die folgenden Ausführungen zeigen knapp, wie die einzelnen **Bewertungskriterien** konkretisiert werden. Bei der **Protokollunterstützung** wurde dies anhand von Standards zur Datenübertragung und einer Browser-Referenzarchitektur(GG05) durchgeführt. Die Details der (Auszeichnungs-)**Sprachenunterstützung** wurden mit Hilfe einer Analyse aktueller und künftiger Web-Standards sowie der Berücksichtigung des SAGA-Standards ermittelt. Relevante **Medientypen** ergaben sich aus der obigen Browser-Referenzarchitektur, aus der Wikimedia MIME-Type Statistik[113], aus einer Statistik[114] für RIA und aus dem sehr umfangreichen HTTP-Archiv[115]. Die Konkretisierung der **Sicherheitsmaßnahmen** erschließt sich aus gängigen Sicherheitslücken von Web-Anwendungen[116], den oben genannten BSI-Dokumenten und den CVE-Datenbanken.

Die Geschwindigkeit des Browserstarts hängt stark von den gewählten Erweiterungen ab – je mehr und komplexere Erweiterungen geladen werden, desto länger dauert der Start. Ohne Erweiterungen starten die drei Alternativen in etwa gleich schnell. Auch beim Darstellen und Ausführen von JavaScript-Inhalten weisen die getesteten Alternativen keine allzu großen Unterschiede auf[117] und geben die benötigten Ressourcen nach dem Schließen von Webseiten allesamt wieder zurück. Auf eine gesonderte Bewertung dieser Performance-Aspekte wird daher verzichtet. Die Ergebnisse der übrigen Teile dieser Analyse sind in Tabelle 4.9 zu sehen. Nachdem die aktuell relevanten Ausprägungen der Kriterien bestimmt sind, wird zunächst der IE 9, danach der Firefox 4 und abschließend der Safari 5 getestet.

##### 4.3.2.5.1 Microsoft Internet Explorer 9 (IE9)

Der IE 9 steht für Microsoft Windows Vista und Windows 7 zur Verfügung und unterstützt die **Protokolle** HTTP 1.0/1.1, HTTPS und FTP ausreichend. Bei der Bewertung der **Sprachenunterstützung** zeigte

[111] z.B. http://www.w3b.org/hintergrund/methodik.html, abgerufen: 14.03.2011
[112] siehe u.a. (Die11b), Kap. 6.1.1 Webbrowser
[113] http://commons.wikimedia.org/wiki/Commons:MIME_type_statistics, abgerufen: 18.03.2011
[114] http://www.riastats.com/, abgerufen: 18.03.2011
[115] http://httparchive.org/interesting.php, abgerufen: 01.04.2011
[116] Zum Beispiel http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project oder http://www.sans.org/top25-software-errors, abgerufen: 16.03.2011
[117] siehe u.a. http://crockford.com/javascript/performance.html, abgerufen: 26.4.2011

der IE 9 bei HTML 4.01 laut Test-Suite[118] Schwächen. Ähnlich erging es ihm bei der HTML 5 Test-Suite[119], bei der der Browser im Vergleich zu den anderen Probanden schlechter abschneidet. XHTML 1.0 ist eine Obermenge von HTML 4.01[120]; die über letztere hinausgehenden Bestandteile handhabt der Browser als entsprechenden MIME-Typen und bietet einen adäquaten Support[121]. Die nicht lückenlose CSS 2.1 Unterstützung[122] führt zwar zum Punktabzug, behindert aber kaum das Surfen im Internet. CSS 3 wird ebenfalls nicht vollständig unterstützt[123]. Dies führt nur zu einer kleinen Abwertung, zumal die dritte Version der Stylesheet-Sprache noch nicht standardisiert ist. Ein Vergleich zwischen den drei Probanden bezüglich CSS 3 zeigt in der Summe keine wesentlichen Unterschiede[124], d.h. eine weitere Abwertung ist hier nicht nötig. Detailliert kann die CSS-3-Unterstützung des IE 9 nicht mit anderen Browsern verglichen werden, da noch nicht klar ist, welche Sprachelemente der Stylesheet-Sprache stärker zu gewichten bzw. überhaupt relevant sind.

Der IE 9 bietet hinsichtlich seiner **Erweiterbarkeit** verschiedene Möglichkeiten[125]. Neben der Anpassung des Aussehens und Verhaltens (*Browser Extensions*) können sogenannte *Content Extensions* zur Darstellung weiterer Medientypen erstellt werden. Die Spezifikation zum Erstellen solcher Browser-Erweiterungen ist frei zugänglich, Erweiterungen können signiert und als „Sicher für Skripting“ markiert werden. Der Browser wiederum kann (ggf. behördenweit per Gruppenrichtlinie) für jede Webseite so eingestellt werden, dass er nur solcherart markierte oder ggf. gar keine Erweiterungen ausführt. Der Schutz des Browsers vor randalierenden oder bösartigen Erweiterungen beschränkt sich ansonsten auf eine Sammlung von Tipps, wie man möglichst stabile Erweiterungen schreibt[126].

Bei den **Medientypen** stellt der Proband JPEG (ISO/IEC 10918), PNG 1.2 und GIF v89a problemlos dar. Zur Darstellung aktiver Inhalte wie Flash (SWF), Silverlight und Java-Applets stehen für den IE 9 Erweiterungen bereit. Auch JavaScript-Support ist über die JavaScript-Engine gegeben. PDF (per Erweiterung), Atom und RSS unterstützt der Browser ebenfalls.

Neben den oben genannten Einstellmöglichkeiten für aktive Inhalte bietet der IE 9 weitere **Sicherheitsmaßnahmen**. Beim Malware- und Phishing-Schutz schneidet der neue Microsoft-Browser dank des SmartScreen-Filters sehr gut ab(NSS10). Ein bedingtes Ein- bzw. Abschalten von JavaScript zum Schutz gegen JavaScript-basiertes Cross-Site-Scripting (XSS) ist ebenfalls komfortabel möglich. Auch der integrierte XSS-Filter ist zu erwähnen, der vor reflexiven XSS und XSS über CSS schützt[127]. Des weiteren bietet der IE 9 per Black- und White-Listen umfangreichen Tracking-Schutz. Dadurch ist ein individuelles Ausfiltern von Zählpixeln, Google-Analytics-Skripten o.ä. durchführbar(BB11). Das sogenannte „Private Surfen“ erlaubt der Browser ebenfalls.

#### 4.3.2.5.2 Mozilla Firefox 4

Firefox 4 als nächster Proband steht auf allen relevanten Plattformen zur Verfügung und bietet ebenfalls eine ausreichende Unterstützung für die **Protokolle** FTP, HTTP 1.0/1.1 und HTTPS. Bei der **Sprachunterstützung** zeigt der neue Mozilla Browser den gleichen HTML-4.01-Fehler wie der IE 9, bietet aber ebenfalls eine gute Unterstützung der Auszeichnungs-Sprache. Bei der HTML-5-Test-Suite schneidet er beinahe doppelt so gut ab wie der IE9 und auch etwas besser als Safari 5. Bei den berücksichtigten XHTML-Tests liefert der Browser sehr ähnliche Ergebnisse wie der IE 9. CSS 2.1 wird ebenfalls nicht vollständig durch die Layout-Engine unterstützt[128]. Trotzdem steht einem problemlosen Surfen kaum et-

[118] http://www.w3.org/MarkUp/Test/HTML401/current/tests/sec6_16-BF-01.html, abgerufen: 31.03.2011
[119] http://html5test.com/index.html, abgerufen: 31.03.2011
[120] http://www.w3.org/TR/2001/REC-xhtml11-20010531/, abgerufen: 31.03.2011
[121] http://www.w3.org/MarkUp/Test/xhtml-print/current/xhtml_conform_testlist.htm, abgerufen: 31.03.2011
[122] http://msdn.microsoft.com/en-us/library/gg558088(v=VS.85).aspx, abgerufen: 31.03.2011
[123] http://msdn.microsoft.com/en-us/library/cc351024(v=vs.85).aspx, abgerufen: 31.03.2011
[124] http://en.wikipedia.org/wiki/Comparison_of_layout_engines_(Cascading_Style_Sheets) oder http://tools.css3.info/selectors-test/test.html, abgerufen: 31.03.2011
[125] siehe http://msdn.microsoft.com/en-us/ie/aa740475, abgerufen: 27.04.2011
[126] siehe http://msdn.microsoft.com/library/aa753617.aspx, abgerufen: 27.04.2011
[127] http://www.browserscope.org/, Mit IE 9 und Standardeinstellungen durchgeführt, abgerufen: 04.04.2011
[128] https://developer.mozilla.org/de/CSS/CSS_Unterst%C3%BCtzung, abgerufen: 01.04.2011

was im Weg. Die CSS-3-Unterstützung wird genauso bewertet wie beim IE 9, da dort bereits gezeigt wurde, dass die Summe der berücksichtigten Elemente in etwa gleich ist.

Für Flash, Silverlight und Java-Applets, die im Rahmen der **Medientypenunterstützung** relevant sind, existieren aktuelle Erweiterungen. JavaScript rendert der Browser durch die in Version 2 erschiene Layout-Engine Gecko. Auch JPEG, PNG 1.2 und GIF v89a stellt der Firefox 4 problemlos dar. Zur Präsentation von PDF-Dokumenten stehen diverse Erweiterungen bereit. RSS und Atom-Feeds können über den integrierten Betrachter gelesen werden. Die **Erweiterbarkeit** von Firefox ist umfassend; analog zum IE 9 können durch sog. *Extensions* oder *Add-Ons* sowohl das Aussehen und Verhalten geändert als auch die Darstellung weiterer Medientypen ermöglicht werden. Eine Dokumentation zur Erstellung von Erweiterungen ist vorhanden. Mozilla bietet selbst sehr viele Erweiterungen an[129]; der Browser ist allerdings vor randalierenden oder bösartigen Plug-Ins genauso gut oder wenig geschützt wie der IE 9. Immerhin kann man die Installation von Erweiterungen behördenweit administrieren und ggf. unterbinden.

Als **Sicherheitsmaßnahme** gegen Malware und Phishing geht der Firefox einen ähnlichen Weg wie der IE 9, prüft URLs über Datenbankabfragen auf potentiell gefährliche Inhalte und zeigt ggf. Warnungen an. Firefox verwendet zur Datenbankabfrage die Safe-Browsing-API von Google, die allerdings im Test(NSS10) deutlich weniger problematische Seiten erkennt als Microsofts SmartScreen-Filter. Zwar wurde dort der Firefox 3.6 getestet, doch der verwendete Google-Dienst bleibt auch bei Firefox 4.0 derselbe und somit auch dessen Qualität hinsichtlich erkannter Malware- und Phishing-Seiten. Folglich wird der Mozilla-Browser gegenüber dem IE 9 hier schlechter bewertet.

Einen integrierten XSS-Schutz bietet der Firefox nicht. Somit ist er anfällig für reflexive XSS-Angriffe[130], was zu einer Abwertung gegenüber dem IE 9 und Safari 5 führt. Zu Beachten ist hier allerdings, dass mit NoScript eine etablierte Erweiterung bereitsteht, die dieses Problem behebt[131]. Zusätzlich dazu schlägt die Mozilla Foundation Content Security Policy (CSP) als Sicherheitskonzept gegen XSS-Attacken vor[132]. Hier bleibt abzuwarten, ob sich dieses Vorgehen durchsetzt.

Um den Anwender vor Tracking zu schützen, schlagen die Firefox-Hersteller zusätzlich zu den Erweiterungen „AdBlock Plus“ oder „Ghostery“[133] den Weg ein, bei jedem HTTP-Request einen Do-Not-Track-Header mitzusenden. Die Folge davon soll sein, dass der Anbieter von Webinhalten bei gesetztem Header keine Nutzerdaten speichert. Auch hier bleibt abzuwarten, ob sich dieses Konzept durchsetzt, denn dazu müssen die Seiteninhaber natürlich mitspielen. Erste Erfolge wurden allerdings bereits verzeichnet[134]. Die Option zum privaten Surfen bietet der Browser ebenfalls an.

#### 4.3.2.5.3 Apple Safari 5

Safari 5 steht für Apple Mac OS X und die Windows-Versionen XP, Vista und 7 zur Verfügung und zeigt bei der **Protokoll**-, **Sprachen**- und **Medientypenunterstützung** annähernd die gleichen Ergebnisse wie die beiden vorhergehenden Probanden. Auch die **Erweiterbarkeit** ist über *Plug-Ins* und *Extensions* gegeben, denen zur Sicherheit jeweils ein Zertifikat von Apple beiliegen muss. Das Zertifikat wird erst nach entsprechender Überprüfung der Erweiterung ausgestellt. Dies erschwert das Unterschieben von Schadsoftware. Plug-Ins werden auf 64-Bit-Plattformen in eigenen Prozessen ausgeführt, was das Übergreifen auf andere Browser-Bereiche oder das Abstürzenlassen des Browsers durch fehlerhafte Plug-Ins wirksam verhindert. Eine Dokumentation wie Erweiterungen zu Erstellen sind, liegt auf der Apple-Webseite vor.

---

[129] siehe https://addons.mozilla.org/de/firefox/

[130] http://www.browserscope.org/, mit Firefox 4.0 und Standardeinstellungen durchgeführt, abgerufen: 04.04.2011

[131] http://www.browserscope.org/, Mit Firefox 4.0 und Standardeinstellungen + NoScript 2.1.0.1 und Standardeinstellungen durchgeführt, abgerufen: 04.04.2011

[132] http://www.heise.de/security/meldung/Erste-Firefox-Demo-fuer-Content-Security-Policy-807720.html, abgerufen: 04.04.2011

[133] https://www.datenschutzzentrum.de/tracking/schutz-vor-tracking.html, abgerufen: 01.04.2011

[134] http://www.golem.de/1102/81280.html, abgerufen: 01.04.2011

Bei den **Sicherheitsmaßnahmen** gegen Malware und Phishing setzt auch Safari 5 auf den Safe-Browsing-Dienst von Google, schneidet allerdings noch schlechter ab als der Firefox(NSS10). Der integrierte XSS-Schutz schützt vor reflexiven XSS und XSS über CSS. Hierfür ist keine Erweiterung nötig, d.h. der Browser wird hier besser bewertet als der Firefox 4. Das Fehlen des seitenspezifischen Ausführens von JavaScript führt dazu, dass der Apple-Proband schlechter abschneidet als der IE 9. Ein integrierter Tracking-Schutz fehlt dem Browser ebenfalls. Dafür sind die bereits erwähnten Erweiterungen AdBlock Plus und Ghostery verfügbar. Eine Option zum privaten Surfen bietet der Browser an.

#### 4.3.2.6 Bewertungstabelle

Tabelle 4.9: Vergleich Web-Browser

| Browser | Firefox 4 | IE 9 | Safari 5 |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | ✓ | - | ✓[135] |
| Unterstützte Plattformen<br>Windows XP / Windows 7 / Linux / MacOS X | ✓/✓/✓/✓ | -/✓/-/- | ✓/✓/-/✓ |
| **Grundfunktionen** | | | |
| Protokollunterstützung<br>HTTP 1.0,1.1 / HTTPS / FTP | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| Sprachenunterstützung<br>HTML 4.01 / HTML 5 / XHTML 1.0 / CSS 2.1 / CSS 3 | +/+/+/+/++ | +/o/+/+/++ | +/+/+/+/++ |
| **Medientypenunterstützung** | | | |
| Aktive Inhalte<br>MS Silverlight / Adobe Flash / Java-Applets (JVM 1.6) / JavaScript 1.8.5 (inkl. XMLHttpRequestObject) | ✓/✓/✓/✓ | ✓/✓/✓/✓ | ✓/✓/✓/✓ |
| Bild- und Grafikformate<br>JPEG / PNG 1.2 / GIF v89a | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| Dokumentenformate<br>PDF 1.7 / RSS / Atom | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| **Sonstige Merkmale** | | | |
| Erweiterbarkeit<br>Aussehen u. Verhalten / weitere Medientypen / Dokumentation / Plug-In-Sicherheit | ✓/✓/✓/- | ✓/✓/✓/- | ✓/✓/✓/++ |
| Sicherheitsmaßnahmen<br>Malware / Phishing / XSS / Tracking / Privates Surfen | o/o/-/+/✓ | ++/++/+/+/✓ | -/-/o/+/✓ |
| **Bewertung** | | | |
| Protokollunterstützung | ++ | ++ | ++ |
| Unterstützte Sprachen | ++ | + | ++ |
| Medientypenunterstützung | ++ | ++ | ++ |
| Sicherheitsmaßnahmen | o | + | o |

[135] Safari verwendet die OSS-Rendering-Enginge WebKit

#### 4.3.2.7 Empfehlungen

Die betrachteten Browser unterstützen alle wesentlichen Internet-Standards und Medientypen, sind nahezu beliebig erweiterbar und enthalten ähnliche Sicherheitskonzepte. Sie sind daher für den Behördeneinsatz grundsätzlich geeignet. Allerdings bietet nur der Firefox eine Verfügbarkeit auf sämtlichen relevanten Betriebssystemen und aufgrund seiner Open-Source-Politik die verlässlichste Gewähr dafür, dass er dauerhaft offene Standards unterstützt und eigene Sonderwege vermeidet.

Sofern noch keine behördenweite Festlegung auf einen bestimmten Browser getroffen wurde, sollte dies nun für die Zukunft nachgeholt werden. Eine solche Festlegung vereinfacht die Administration der Arbeitsplatzrechner und erleichtert die Bereitstellung benötigter Erweiterungen. Zudem kann dadurch der Testaufwand für die grafische Benutzerschnittstelle Browser-basierter Fachanwendungen und für das Intranet-Angebot deutlich reduziert werden. Die Festlegung auf einen bestimmten Browser sollte sich an den vorstehenden Kriterien orientieren und nicht etwa daran, ob ein anderer als der gewünschte Browser bereits im System vorhanden ist. Sind bestimmte Fachverfahren vom abzulösenden Browser abhängig, muss dieser allerdings so lange parallel unterstützt werden, bis die Abhängigkeiten aufgelöst sind.

#### 4.3.2.8 Migrations-Checkliste

Das sequenzielle Durchlaufen der nachfolgenden Checkliste stellt sicher, dass alle relevanten Aspekte bei der Migration eines Webbrowsers berücksichtigt werden. Die unter den Arbeitsschritten stehenden Informationen zeigen, wie die Bewertungskriterien konkretisiert werden können.

##### 4.3.2.8.1 Derzeit meistverwendete Browser-Alternative bestimmen

1. Analyse von Unternehmensrichtlinien
2. Auswertung der HTTP User-Agent-Header Einträge in Server-Log-Files des Intranets

##### 4.3.2.8.2 Ist-Analyse der meistverwendeten Browser-Alternative durchführen bezüglich

1. Protokollunterstützung
   Einsatz von Testsoftware, Sichtung der Herstellerspezifikation, Aufruf von Internet-Testseiten
2. Sprachenunterstützung
   Einsatz von Testsoftware, Sichtung der Herstellerspezifikation, Aufruf von Internet-Testseiten
3. Medientypenunterstützung
   Einsatz von Testsoftware, Sichtung der Herstellerspezifikation, Aufruf von Internet-Testseiten
4. Sicherheitsmaßnahmen
   Sichtung der BSI-Dokumente, Analyse von CVE-Datenbanken, Aufruf von Internet-Testseiten
5. Domänenspezifischer Bewertungskriterien
   z.B. Existieren Fachverfahren die bestimmte Browser-Technologien zur Ausführung benötigen? (Abhängigkeit von ActiveX? Abhängigkeit von bestimmten Browser-Plug-Ins?)

##### 4.3.2.8.3 Soll-Konzeption durchführen bezüglich

1. Protokollunterstützung
   Welche vom SAGA-Standard empfohlenen oder beobachteten Anwendungsprotokolle werden benötigt? Welche sonstigen (ggf. kommenden) Protokolle müssen aus fachlichen Gründen berücksichtigt werden?

2. Sprachenunterstützung
   Welche vom SAGA-Standard empfohlenen oder beobachtetenaktiven Inhalte, Formulare und Technologien zur Informationsaufbereitung werden benötigt? Welche sonstigen (ggf. kommenden) Sprachen wie HTML5 oder CSS3 müssen aus fachlichen Gründen berücksichtigt werden?

3. Medientypenunterstützung
   Welche vom SAGA-Standard empfohlenen oder beobachteten Austauschformate für Daten, Dokumente, Bilder, Animationen, Audiodaten, Videodaten, 3D-Daten und Geoinformationen werden zur Darstellung im Browser benötigt? Welche sonstigen Medientypen müssen aus fachlichen Gründen berücksichtigt werden?

4. Sicherheitsmaßnahmen
   Welche vom BSI empfohlenen Sicherheitsmaßnahmen sind im konkreten Umfeld relevant? Welche CVE-Datenbanken sollen zur Schwachstellenanalyse der Browser-Alternativen ausgewertet werden? Welche sonstigen Maßnahmen zur Schwachstellen-Analyse (z.B. Einholung von Sicherheitsexpertisen) sollen durchgeführt werden? Wird die gewünschte Browser-Alternative häufig mit Sicherheits-Updates versorgt? Kann das Einspielen dieser Sicherheits-Updates ohne Benutzereingriff durchgeführt werden? Können Sicherheitseinstellungen der jeweiligen Browser-Instanzen zentral administriert werden?

5. Domänenspezifika
   Sind die notwendigen Browser-Plug-Ins für Alternativ-Browser verfügbar? Welche Abhängigkeiten (ActiveX, Plug-Ins) müssen für welche Zeit berücksichtigt werden? Gibt es Planungen anderer IT-Projekte des Hauses zu fachspezifischen Browser-Fähigkeiten?

#### 4.3.2.8.4 Bewertung und Entscheidung

1. Vorauswahl der Prüfkandidaten
   Anhand der oben vorgestellten Browser-Alternativen unter Berücksichtigung der jeweils aktuellen Version

2. Gewichtung der Bereiche Protokoll-, Sprachen- und Medientypenunterstützung, Sicherheitsmaßnahmen und domänenspezifische Bewertungskriterien (Summe der Gewichtungen = 100%)

3. Eintragen der Bewertungsergebnisse der Bereiche

4. Ermitteln des Gesamtergebnisses durch Multiplikation der Gewichtung und des Bewertungsergebnisses je Bereich für alle betrachteten Alternativen

### 4.3.3 Personal Information Manager

#### 4.3.3.1 Einleitung

Mit der stark zunehmenden Digitalisierung und Vernetzung der Arbeitsplätze geht der steigende Bedarf an Möglichkeiten einher, persönliche und geschäftlich relevante Kontaktdaten, Termine und Informationen in IT-Systemen zu speichern, zu verwalten und bei Bedarf mit anderen Personen zu teilen. Ein Personal Information Manager (PIM) dient auf Seiten des Anwenders zur Abdeckung dieser Aufgaben, indem er auf einem Groupware-Server verwaltete Informationen bereitstellt und darüber austauscht. Der PIM ist deshalb neben dem Browser ein zentraler Bestandteil eines digitalen Arbeitsplatzes.

#### 4.3.3.2 Kriterienkatalog

Ein PIM dient als Terminkalender und Aufgabenliste und hat dort verschiedene Funktionen zu unterstützen, er muss Kontaktdaten im Adressbuch verwalten und bereitstellen und zum Empfang und Versand von Nachrichten an einen Mailserver angebunden werden (**Grundfunktionalität**). Diese Funktionalitäten basieren auf verschiedenen **Protokollen und Formaten**, die großteils offen standardisiert sind und deren Einhaltung zu prüfen ist. Die **Synchronisation** der gespeicherten Informationen mit anderen Nutzern und Mobilgeräten sowie der **Zugriff** mit anderen PIM sollte möglich sein. Zudem sollten die Informationen den Kriterien der **IT-Sicherheit** gemäß vor unbefügtem Zugriff geschützt sein.

Die Möglichkeit zu **benutzerspezifischen Einstellungen** erhöht den Komfort der jeweiligen Funktionalität und erleichtert die tägliche Arbeit, beispielsweise durch persönliche E-Mail-Filter und -Signaturen. Entsprechende Möglichkeiten sind daher ebenso zu prüfen und zu bewerten wie die **Erweiterbarkeit** eines PIM durch Plug-Ins und deren **Konfigurierbarkeit**.

#### 4.3.3.3 Methodik

Zunächst ist zu klären, welche Teile der Grundfunktionalität durch die Infrastruktur derzeit unterstützt werden. Aufschluss gibt eine Analyse der Häufigkeitsverteilung der aktuell eingesetzten PIM samt verwendeter Komponenten. Der Grad an Abhängigkeit von der serverseitig verwendeten Groupware-Lösung muss in die Analyse einfließen. Um die Häufigkeitsverteilung zu ermitteln, können Unternehmensrichtlinien oder eine Befragung des IT-Verantwortlichen dienen. Ist die Nutzung eines bestimmten PIM nicht bereits in den Richtlinien der IT-Infrastruktur vorgeschrieben, bedarf es einer Erhebung unter den Nutzern.

Die Häufigkeitsverteilung muss Aufschluss über die derzeit verwendeten Protokolle und Formate geben. In einer Erhebung sollte zudem geklärt werden, ob Anforderungen an die Synchronisation zwischen Mobilgeräten und PIM neben der Synchronisierung von Mobilgeräten mit dem Groupware-Server bestehen (zu letzterem siehe Abschnitt 4.2.4). Die derzeit möglichen benutzerspezifischen Einstellungen sind hinsichtlich ihrer Nutzung zu erfassen und zu gewichten. Dasselbe gilt für die aktuellen Möglichkeiten der IT-Sicherheit (verschlüsselte Kommunikation, elektronische Signatur, Einbindung von Virenscannern, etc.).

Der Soll-Zustand muss die Kommunikation mit dem Groupware-Server, dessen Funktionalität, vorgegebene Client-Plattformen und strategische Vorgaben berücksichtigen. Die Grundfunktionalität der bestehenden Groupware muss weiter genutzt werden können. Die aktuellen Möglichkeiten der IT-Sicherheit müssen mindestens fortgeführt und angesichts des kommenden Bürgerportals (DE-Mail) ggf. um das Verschlüsseln und Signieren von E-Mails erweitert werden. Zur Bewertung der **IT-Sicherheit** ist neben der Prüfung einer gesicherten Kommunikation mit dem Groupware-Server und des Erscheinungszyklus sicherheitsrelevanter Updates und Patches ein Abgleich mit einer CVE Datenbank[136] zu empfehlen, die über Sicherheitslücken und Angriffspunkte von Software Auskunft gibt.

Jede Grundfunktion basiert auf spezifischen Protokollen und Formaten. Für E-Mail-Clients relevant sind die offenen Protokolle POP3, IMAP, SMTP und das von Microsoft verwendete proprietäre MAPI. Hin-

[136] Beispiel für eine CVE-Datenbank: http://www.cvedetails.com/

sichtlich IMAP sollte geprüft werden, in welchem Umfang das Protokoll genutzt werden soll, ob zum Beispiel die Rechte zum gemeinsamen Zugriff verschiedener Benutzer auf einen Ordner darüber vergeben werden sollen. Beim Terminkalender muss das Format zum Austausch einzelner Termine mit Dritten geprüft werden. Damit die Synchronisation von Terminen mit anderen Personen, das Verschicken von Einladungen, Erinnerungen und Absagen sowie das Buchen von gemeinsam genutzten Ressourcen reibungslos funktioniert, müssen PIM die dafür relevanten Protokolle und Formate (iCal, CalDAV/WebDAV) unterstützen. Adressbücher sollten in der Lage sein, mehrere unterschiedliche Kontaktlisten unabhängig voneinander zu verwalten, in offenen Formaten zu exportieren und LDAP-Verzeichnisdienste einzubinden.

Die Anforderungen an eine benutzerfreundliche und intuitive Anwenderschnittstelle sowie deren Erweiterbarkeit und Konfigurierbarkeit müssen formuliert und bewertet werden. In die Betrachtung mit einbezogen werden müssen zudem der Ressourcenverbrauch und Möglichkeiten zur Datensicherung. Weitere spezifische Anforderungen an einen PIM können für die Bewertung mit aufgenommen werden.

#### 4.3.3.4 Betrachtete Alternativen

Die Auswahl der betrachteten Alternativen basiert mangels vergleichbarer Absatzzahlen und verlässlicher Erhebungen zu deren Verbreitung auf Schätzungen. Auf dieser Basis werden folgende Produkte beleuchtet:

- **Microsoft Outlook** als Marktführer,
- **Mozilla Thunderbird** als am weitesten verbreiteter OSS-Lösung,
- **Evolution** als weit verbreiteter OSS-Lösung und Standard-PIM in Gnome-Umgebungen sowie
- **Kontact** als ebenfalls weit verbreiteter OSS-Lösung und Standard-PIM in KDE-Umgebungen.

Weiterhin gibt es für die meisten der im Abschnitt 4.2.4 vorgestellten Groupware-Server Web-Frontends, mit denen man per Browser auf die Daten des Servers zugreifen kann. Diese Möglichkeit des Zugriffs wird als Funktionalität der Groupware-Server dort behandelt.

#### 4.3.3.5 Bewertung

Im Folgenden werden die vier ausgewählten PIM auf die o.g. Kriterien hin untersucht und bewertet. Die unterstützte Grundfunktionalität ergibt sich aus der Software selbst, die implementierten Protokolle und Formate leiten sich ebenso wie alle anderen Kriterien aus den Angaben der Hersteller ab, wobei Tests, Erfahrungen und bekannte Probleme mit einfließen. Die Bewertung der IT-Sicherheit ist an die oben erwähnten Datenbanken und bekannten Sicherheitsthematiken angelehnt.

##### 4.3.3.5.1 Microsoft Outlook

Microsoft Outlook[137] ist als Teil der Office-Suite aus demselben Hause weit verbreitet und bietet eine sehr gute Anbindung an den ebenfalls von Microsoft vertriebenen Exchange Server, der wiederum der Marktführer im Bereich der Groupware-Lösungen[138] ist. Outlook kann auch separat ohne die Office-Suite erworben werden.

Outlook bietet im Lieferzustand alle o.g. Grundfunktionen eines PIM und zusätzlich die Möglichkeit, öffentliche Ordner des Exchange Servers anzuzeigen und mittels Rechtevergabe Zugriffe zu erlauben. Die Anbindung an einen Exchange Server erfolgt über das Messaging Application Programming Interface (MAPI), die von Microsoft entwickelte proprietäre Schnittstelle des Exchange Servers. Outlook unterstützt zudem die offenen Protokolle IMAP und SMTP zum E-Mail-Empfang bzw. Versand, so dass serverseitig alternative Groupware-Lösungen eingesetzt werden können.

[137] Betrachtet wurde Outlook 2010.
[138] siehe Kap.4.2.4

Outlook unterstützt die Verwendung mehrerer Mailkonten mit ggf. unterschiedlichen Servertypen und Protokollen (Exchange/IMAP). E-Mails können im Text- oder HTML-Format erstellt und gelesen werden. Daten werden im sogenannten Personal Store (PST) gespeichert, einer Container-Datei mit proprietärem Format, in der Aufgaben, Notizen, E-Mails und Termine abgelegt werden. Dieser PST kann von anderen Programmen (Mailclients etc.) nicht gelesen werden, was ein erhebliches Hindernis beim Wechsel zu einem anderen PIM mit vollständiger Datenübernahme darstellt. Für eine Datensicherung kann eine Kopie der PST-Dateien erstellt werden. Verschiedene Konfigurationen wie Programmeinstellungen, Signaturen usw. werden aber außerhalb des PST gespeichert, so dass diese hier nicht berücksichtigt werden. PST-Dateien sind in ihrer Größe beschränkt[139]; Outlook kann ggf. mehrere PST gleichzeitig nutzen.

Das Produkt bietet Möglichkeiten zum Schutz vor Junk- und Phishing-Mails und zum Verschlüsseln und Signieren von E-Mails bei vorliegendem Anwender-Zertifikat. Außerdem können PST zum Schutz vor unerwünschtem Import durch Dritte mit einem Kennwort versehen werden. Das Aufbauen von verschlüsselten Verbindungen zu den konfigurierten Servern wird unterstützt.

Das Adressbuch kann auf mehrere lokale oder zentrale Datenbasen zugreifen und unterstützt auch eine LDAP-Anbindung. Ausführliche Filterregeln können je Konto definiert werden, eine Suchfunktion wird ebenfalls angeboten. Je Komponente sind viele weitere Einstellungsmöglichkeiten vorhanden. Die Erweiterbarkeit duch Plug-Ins und Add-Ons ist möglich, aber aufgrund der proprietären Natur des Produkts auf wenige Anbieter beschränkt. Ebenfalls nur eingeschränkt möglich ist eine optische Konfiguration, das charakteristische Aussehen von Outlook lässt sich nicht verändern.

Auch wenn Outlook grundsätzlich auch mit alternativen Groupware-Lösungen zusammenarbeitet, ist es doch für den Gebrauch mit Exchange konzipiert. Bei einer Kopplung an andere Groupware-Server können Probleme auftreten. So ist beispielsweise zwar das Importieren von Kalenderdaten im iCal-Format möglich, nicht aber deren unmittelbare Einbindung und Synchronisierung. Beim Mailversand über SMTP verletzt Outlook die Protokollspezifikation, indem es in einigen Kommandos unzulässige Leerzeichen einfügt, was zu zerstückelten E-Mails führen kann. Die meisten Mailserver sehen über diese weit verbreitete Protokollverletzung jedoch hinweg, so dass dadurch nur selten Probleme auftreten.

#### 4.3.3.5.2 Mozilla Thunderbird

Thunderbird ist die Open-Source Software im Bereich der Personal Information Manager mit der größten Benutzergemeinde, wird in Behörden häufig genutzt und hat sich einen festen Platz in der IT-Landschaft gesichert.

Mozilla bietet den E-Mail-Client Thunderbird für alle gängigen Betriebssysteme zum kostenlosen Download an[140]. Thunderbird ist zwar in der Standardversion lediglich ein E-Mail-Client mit Adressbuch, kann aber durch Plug-Ins insbesondere um Kalender und Aufgabenliste erweitert werden. Dazu ist das Plug-In Lightning[141] als Add-On in Thunderbird zu installieren. Es erweitert die Basisversion um die beiden fehlenden Komponenten, so dass fortan die Grundfunktionalität vorhanden ist.

Als Mailclient unterstützt Thunderbird die Protokolle SMTP zum Versand sowie IMAP und POP3 zum Empfang von E-Mails. Die Implementierung des IMAP-Standards ist beschränkt auf den E-Mail-Verkehr eingeschränkt, die o.g. Option zur Ordner-Rechtevergabe nicht vorhanden. Das von Microsoft Exchange verwendete MAPI wird nicht unterstützt und kann auch durch die Installation von weiteren Plug-Ins nicht hinzugefügt werden. Soll Thunderbird mit einem Microsoft Exchange Server kommunizieren, muss dort folglich der IMAP-Zugriff explizit freigeschaltet werden. Thunderbird unterstützt E-Mails im Text- und im Hypertext Markup Language (HTML)-Format und zeigt beide fehlerfrei an. Der Editor bietet alle benötigten Funktionen, um Mails in der gewünschter Form einfach und schnell zu formatieren.

Die Verbindung zum Server kann sowohl ohne Verschlüsselung als auch StartTLS- oder SSL/TLS-verschlüsselt hergestellt werden. Das Verschlüsseln und Signieren von E-Mails ist individuell und per

[139] Beschränkung bis zu Outlook 2002 auf 2GB, ab Outlook 2003 auf 20GB, ab Outlook 2010 auf 50GB.
[140] Betrachtet wurde die Version 5.0
[141] Die Installation von Lightning kann direkt aus Thunderbird heraus über das Add-Ons Menü durchgeführt werden.

Knopfdruck aus dem Editor heraus möglich, sofern zuvor ein persönliches Benutzerzertifikat installiert wurde. Ein interner Filter für Junk-Mails ist vorhanden und kann mit der Zeit vom Benutzer trainiert werden, um unerwünschte E-Mails selbständig zu erkennen. Eine Warnung vor Scam-Mails mit betrügerischem Inhalt durch Thunderbird kann aktiviert und einem Virenscanner die Erlaubnis erteilt werden, möglicherweise infizierte Mails in die Quarantäne zu verschieben.

Das in Thunderbird integrierte Adressbuch bietet die Möglichkeit, Kontaktdaten in unterschiedliche Kategorien zu unterteilen. In jedem dieser Adressbücher können einzelne Kontakte oder Mailinglisten angelegt werden. Außerdem besteht die Möglichkeit, zentrale Verzeichnisse per LDAP einzubinden. Diese Verbindung kann SSL-verschlüsselt hergestellt werden. Die im LDAP vorhandenen Kontakte können per Knopfdruck auch Offline verfügbar gemacht werden, so dass auch ohne Netzverbindung auf die Kontaktdaten zugegriffen werden kann.

Das Add-On Lightning des Mozilla Calendar Projects mit Kalender und Aufgabenliste[142] integriert sich gut in die Benutzeroberfläche. Es ermöglicht das Anlegen und Verwalten mehrerer lokaler, über das Netz abonnierter oder importierter Kalender und Termine in verschiedenen Kategorien. Dabei beherrscht Lightning mit iCal (.ics) und WebDAV die gängigen offenen Formate und Protokolle. Zusätzlich kann man noch das Sun Java System Calendar Server Format (WCAP / Web Calenar Access Protokoll) auswählen. Wie gut die Synchronisation der externen Kalender mit dem Server funktioniert, hängt stark von der verwendeten Groupware ab; bei den im Migrationsleitfaden betrachteten Groupware-Alternativen traten in Tests keine Probleme auf. In der Aufgabenliste können Items mit Priorität und Fälligkeitsdatum lokal erstellt werden; eine Ablage der Aufgabenliste auf einem Groupware Server wird nicht unterstützt.

In Thunderbird ist die Einrichtung und Konfiguration mehrerer voneinander unabhängiger Mailkonten mit jeweils völlig verschiedenen Einstellungen möglich, deren Bedienung gestaltet sich intuitiv und benutzerfreundlich. Eine automatische Server-Suche erleichtert unerfahrenen Benutzern das Anlegen eines E-Mail-Kontos deutlich. Mailkonten können individuell und weitgehend konfiguriert werden. Es können umfangreiche Filterregeln je Konto definiert werden, das Taggen und Priorisieren von E.Mails ist ebenso möglich.

Die Suchfunktion bietet eine schnelle Suche nach umfangreichen Kriterien, die bei zu vielen Treffern noch per Mausklick nachträglich eingeschränkt werden kann. Mithilfe tausender von Add-ons, die direkt aus dem Programm heraus installiert werden können, kann Thunderbird ganz nach den eigenen Wünschen erweitert werden. Mozilla bietet zur Auswahl und Bewertung der Add-Ons entsprechende Übersichten[143]. Die Optik ist individuell anpassbar und kann ganz auf die Benutzerwünsche abgestimmt werden. Menüleisten können entfernt, hinzugefügt und konfiguriert werden, verschiedene Themes erlauben Farb- und Formenwechsel. Ein „Activity Manager“ und eine Fehlerkonsole loggen die duchgeführten Aktivitäten und Fehler und zeigen diese in übersichtlicher Form an.

Der Ressourcenverbrauch ist gering, weshalb Thunderbird auch auf weniger leistungsstarken Rechnern schnell und zuverlässig agiert. Thunderbird wird von der Mozilla Foundation kontinuierlich verbessert und weiterentwickelt. Daher ist davon auszugehen, dass Thunderbird ein wichtiger Vertreter innerhalb des Bereichs der Personal Information Manager bleibt.

#### 4.3.3.5.3 Evolution

Evolution[144] ist ein frei verfügbarer PIM, der für Linux und andere unixoide Systeme entwickelt wurde. Evolution wurde im Jahr 2000 von der Firma Ximian veröffentlicht, seit der Übernahme der Firma 2003 ist es ein Novell-Produkt. Evolution gilt als am weitesten verbreiteter PIM in Linux-Umgebungen und wird deshalb in diesem Kapitel auch mit in die engere Auswahl einbezogen. Evolution ist zwar als Standard in der Desktopumgebung Gnome integriert und wird zusammen mit dieser weiterentwickelt, ist aber auch für alle anderen Plattformen verfügbar[145].

[142] Betrachtet wurde Lightning 1.0b4 für Thunderbird 5.0
[143] https://addons.mozilla.org/de/thunderbird/
[144] Betrachtet wurde Version 3.0.0.
[145] Auf Windows und MacOS leider nicht immer in der aktuellen Version

Wie Outlook verfügt Evolution bereits in der Standardversion über einen sehr großen Funktionsumfang und enthält mit E-Mail, Kalender, Adressbuch und Aufgabenliste alle Grundfunktionen. Bemerkenswert ist die hervorragende Einbindung in den Gnome-Desktop, der an vielen Stellen auf die im PIM konfigurierten Funktionen zugreift. E-Mails können über IMAP oder POP3 abgerufen und per SMTP versandt werden. Evolution kann sich mit einem Exchange Server über dessenh WebDAV-Schnittstelle verbinden[146]. Nach der Installation des Erweiterungs-Pakets *evolution-mapi* kann die MAPI-Schnittstelle von Exchange genutzt werden, über das Erweiterungspaket *evolution-kolab* wird Evolution zu einem vollständigen Kolab-Client (siehe Abschnitt 4.2.4.

E-Mails können lokal in verschiedenen offen standardisierten Mailbox-Formaten abgelegt werden. Das Einrichten verschiedener Konten wird durch einen Assistenten unterstützt. Umfangreiche Filterregeln können je E-Mail-Account für eingehende Nachrichten angelegt werden, mit denen E-Mails automatisch sortiert, weitergeleitet oder mit Labels versehen werden. Ausgehende E-Mails können priorisiert werden. Praktisch ist, dass beim Verfassen einer Nachricht zwischen verschiedenen gespeicherten Signaturen ausgewählt werden kann.

Verbindungen zu Groupware-Servern können mittels SSL/TLS abgesichert und E-Mails per PGP und S/MIME auf Knopfdruck verschlüsselt und signiert werden. Um unerwünschte Mails im Posteingang zu vermeiden, kann ein Junk-Filter angelernt und ein lokal installierter Spamfilter wie SpamAssasin eingebunden werden.

Der Kalender ermöglicht das Einrichten mehrerer lokaler Kalender und das Einbinden entfernter Kalender über alle gängigen Protokolle. Ein Assistent unterstützt diese Vorgänge und bietet bei der Einbindung entfernter Kalender weitere Hilfen wie die Auswahl zwischen verschiedenen Unterkalendern. So kann per CalDAV mit Google oder anderen Kalendern synchronisiert werden, Termine können definierten Kategorien zugeordnet und mit Erinnerungsfunktionen versehen werden.

Kontakte werden im Adressbuch lokal gepflegt oder vom LDAP-Server geholt. Weitere Optionen sind der direkte Import von Google, per WebDAV oder CouchDB auch von anderen Quellen. Evolution ermöglicht zudem den Import von Tasks (Aufgaben) und Memos (Notizen) per Webcal und CalDAV.

#### 4.3.3.5.4 Kontact

Kontact ist das Pendant zu Evolution in der Desktop-Umgebung KDE und entsprang der Absicht, auch dort einen eigen- und vollständigen Personal Information Manager zu integrieren, der die bereits vorhandene Software bündelt und alle Grundfunktionen eines PIM zusammengefasst in die Desktopumgebung integriert. Dessen Teilbereiche können weiterhin auch außerhalb von Kontact als eigene Anwendung gestartet werden. Dieser modulare Aufbau ermöglicht die Entwicklung weiterer Module oder Anwendungen, ohne Kontact dafür zu ändern. Dadurch können von Dritten entwickelte Plug-Ins eingebunden und so der PIM eigenen Bedürfnissen angepasst werden.

Neben den Grundfunktionen sind weitere Komponenten verfügbar, mit denen zum Beispiel Haftnotizen für den Desktop verwaltet werden können oder protokolliert werden kann, wie viel Zeit für die Erledigung einer Aufgabe benötigt wurde. Eine frei konfigurierbare Zusammenfassung aller wichtigen Inhalte des Tages ist im PIM ebenfalls enthalten.

KMail als E-Mail-Komponente unterstützt die Protokolle IMAP, POP3 und SMTP zum Empfang und Versand von E-Mails. E-Mails können im Text- und HTML-Format erstellt und automatisch oder explizit auf Rechtschreibung geprüft werden. E-Mails können durch Inline OpenPGP, PGP/MIME und S/MIME verschlüsselt und die Kommunikation mit dem Groupware-Server per SSL und TLS abgesichert werden. Wie bei Evolution können gängige Spamfilter wie SpamAssassin oder Bogofilter integriert werden. Ein optionaler Spam-Wahrscheinlichkeitsmeter hilft zudem bei der Erkennung von Spam-Mails.

KOrganizer als Kalender-Komponente von Kontact stellt einen vollständigen Kalender zur Verfügung. Das Verwalten mehrerer lokaler und entfernter Kalender ist möglich und mit den restlichen Funktionalitäten von Kontact integriert.

[146] Derzeit sind Verbindungen bis zu Exchange 2007 darüber möglich.

Eine Aufgabenliste ist zwar nicht vorhanden, jedoch können stattdessen ein Notizbuch (KJots), Haftzettel-Notizen (KNotes) oder der KTimeTracker verwendet werden, mit dem (Unter-)Aufgaben angelegt und diese in einer Art Projektplanung mit Zeitstempel verwaltet werden können.

In Hinblick auf Optik und Haptik kann Kontact mit Thunderbird nicht mithalten, bietet dem Benutzer aber ausreichende Möglichkeiten zur Anpassung des Look and Feel. Die Stärken von Kontact liegen wie bei Evolution in der Integration in die eigene Desktopumgebung und der Unterstützung offener Standards.

#### 4.3.3.6 Bewertungstabelle

Tabelle 4.10: Vergleich Personal Information Manager

| PIM | Outlook | Thunderbird | Evolution | Kontact |
|---|---|---|---|---|
| **Metainformationen** | | | | |
| OSS-Lizenz | – | ✓ | ✓ | ✓ |
| Unterstützte Plattformen (Windows XP / 7 / Linux / MacOS X) | ✓/✓/–/✓ | ✓/✓/✓/✓ | –/–/✓/–[147] | –/–/✓/–[148] |
| **E-Mail** | | | | |
| IMAP/POP3/SMTP | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| MAPI | ✓ | – | ✓[149] | – |
| SSL/TLS | ✓ | ✓ | ✓ | ✓ |
| Verschlüsselung/Signieren | ✓/✓ | ✓/✓ | ✓/✓ | ✓/✓ |
| Filter | ✓ | ✓ | ✓ | ✓ |
| Schutz vor unerwünschten Mails | ✓ | ✓ | ✓ | ✓ |
| Rechtschreibprüfung | ✓ | ✓ | ✓ | ✓ |
| **Kalender** | | | | |
| PIM Integration | ✓ | ✓[150] | ✓ | ✓ |
| iCal/WebDAV/calDAV | ✓/✓/✓[151] | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| **Adressbuch** | | | | |
| PIM Integration | ✓ | ✓ | ✓ | ✓ |
| LDAP | ✓ | ✓ | ✓ | ✓ |
| **Aufgabenliste** | | | | |
| PIM Integration | ✓ | ✓[150] | ✓ | ✓ |
| Serveranbindung | ✓ | – | ✓ | ✓ |
| **Erweiter- und Konfigurierbarkeit** | | | | |
| Plug-Ins | – | ✓ | ✓[152] | ✓ |
| Benutzeroberfläche | – | ✓ | ✓[152] | ✓ |

[147] Veraltete Versionen für Windows und MacOS vorhanden, werden aber nicht mehr gepflegt
[148] Versionen für Windows und MacOS in experimentellem Stadium ohne Produktionsreife vorhanden
[149] Nach Installation des Pakets evolution-mapi
[150] Durch das Plug-In Lightning
[151] Import und Export möglich, bidirektionale Synchronisation erfordert u.U. Zusatzsoftware
[152] Durch die Installation zusätzlicher Pakete im Betriebssystem

#### 4.3.3.7 Empfehlungen

Die betrachteten Personal Information Manager decken alle Grundfunktionalitäten ab und können durchweg über offene Standards mit Groupware-Lösungen und Verzeichnisdiensten verbunden werden. Auf allen relevanten Betriebssystemen ohne Abstriche verfügbar ist aber nur Thunderbird. Outlook kommt nur unter Windows und MacOS in Betracht und bietet nur in Verbindung mit dem Exchange Server wesentliche Vorteile. Evolution und Kontact sind de facto auf Linux beschränkt. Bei der Entscheidung müssen daher sowohl die künftige Client-Plattform als auch der aktuelle und künftige Groupware-Server einbezogen werden.

Die Abkehr von der proprietären MAPI-Schnittstelle durch die Umstellung der Kommunikation auf offene Protokolle ist in jeder Konstellation sinnvoll, da hierdurch Entscheidungsspielraum beim Einsatz von PIM- und Groupware-Lösungen zurückgewonnen werden kann. Zudem ist über offene Protokolle beispielsweise die Einbindung externer Kalenderdienste möglich. Ebenfalls mit mehr Wahlfreiheit bei PIM verbunden ist die Abkehr vom proprietären Personal-Storage-Format (PST). Werden beide Maßnahmen umgesetzt, können eine Herstellerbindung vermieden und dadurch prinzipiell Kosten gesenkt werden. Zudem wird dadurch der Weg für weitere Migrationsmaßnahmen wie eine Umstellung oder Auslagerung der Groupware bereitet.

#### 4.3.3.8 Migrations-Checkliste

Für die Migration im Bereich PIM kann man durch Einhaltung der unten aufgeführten Checkliste sicherstellen, dass alle relevanten Aspekte berücksichtigt werden.

##### 4.3.3.8.1 Ist-Analyse durchführen

1. Aktuell verwendete PIM samt Version und genutzten Komponenten
2. Eingesetzte Groupwarelösung(en)
3. Genutzte Client-Plattformen
4. Domänenspezifische Bewertungskriterien

##### 4.3.3.8.2 Ist-Analyse auswerten

1. Liste mit geforderten Grundfunktionalitäten
2. Liste mit spezifischen Zusatz-Anforderungen
3. Priorisierung der Anforderungen
4. Auswertung und Konsolidierung

##### 4.3.3.8.3 Soll-Konzeption durchführen

1. Festlegen der relevanten PIM-Bestandteile
2. Festlegen der relevanten Client-Arten (Offline- und Mobil-Fähigkeiten)
3. Festlegen der relevanten Kommunikations-Protokolle
4. Festlegen der Sicherheitsanforderungen
5. Domänenspezifika festlegen

#### 4.3.3.8.4 Bewertung und Entscheidung

1. Vorauswahl der Prüfkandidaten
   Anhand der oben vorgestellten Alternativen unter Berücksichtigung der Groupwarelösung und des eingesetzten Betriebssystems
2. Abgleich der Anforderungen an die Basisfunktionalität mit Funktionalitäten der Produkte
3. Abgleich der spezifischen Zusatz-Anforderungen mit Funktionalitäten der Produkte
4. Prüfung von Migrationsmöglichkeiten
5. Gewichtung der Bereiche Basisfunktionalität, Formatunterstützung, und domänenspezifischer Bewertungskriterien

### 4.3.4 Office-Suiten

#### 4.3.4.1 Einleitung

Office-Suiten sind Produkte mit Komponenten zur Erstellung, Bearbeitung und Speicherung elektronischer Dokumente. Je nach Produkt, Version und Lizenz können unterschiedliche Komponenten enthalten sein; die Bereiche Textverarbeitung, Tabellenkalkulation und Präsentation gehören aber stets dazu, werden daher auch Basiskomponenten genannt und sind Gegenstand der Betrachtungen dieses Abschnitts.

Seit der Veröffentlichung des letzten Migrationsleitfadens sind für die dort betrachteten Produkte Microsoft Office und OpenOffice.org[153] jeweils neue Versionen erschienen. Im Zuge der Übernahme von SUN und damit auch von OpenOffice.org durch Oracle wurde die Abspaltung LibreOffice unter der dazu gegründeten Document Foundation[154] geschaffen, die inzwischen von allen großen Linux-Distributoren als Ersatz für OpenOffice.org verwendet wird. Oracle wiederum hat OpenOffice.org inzwischen an die Apache Foundation übergeben. Ob Open- und LibreOffice bald wieder vereinigt werden oder konkurrierende Produkte bleiben, ist derzeit nicht abzusehen. Die Unterschiede in den derzeit stabilen Versionen sind noch gering (BN11), eine gesonderte Betrachtung beider Varianten erscheint daher nicht geboten. Im weiteren Text wird der besseren Lesbarkeit halber LibreOffice als Oberbegriff für beide Varianten verwendet.

Außerdem wurde zwischenzeitlich die Stelle des/der Beauftragten der Bundesregierung für Informationstechnik nebst untergeordneten Gremien geschaffen, die bereits eine Vielzahl von für die Verwaltung verbindlichen Beschlüssen gefasst haben. Einer davon, der IT-Rats-Beschluss Nr. 11/2008 (Rat08), berührt die Betrachtung von Office-Suiten unmittelbar, da er den Mindestumfang der Verwendung des OASIS Open Document Format for Office Applications (ODF) klar vorgibt:

> „Zur Verwirklichung eines diskriminierungsfreien E-Governments muss sich die Bundesverwaltung in die Lage versetzen, Dokumente in diesem Format empfangen, bearbeiten, erzeugen und versenden zu können."

Folglich ist bei einer Migrationsentscheidung die Konformität des jeweiligen Produkts zu diesem Standard von wesentlicher Bedeutung. Allerdings spielen auch verschiedene andere Aspekte wie genutzte und erwartete Funktionalität oder die Verwendung aktiver Inhalte eine gewichtige Rolle. Außerdem gilt es, Erfahrungen aus diesbezüglichen Migrationsprojekten wie dem Münchner LiMux-Projekt[155] zu berücksichtigen und dort gefundene Lösungswege aufzuzeigen.

#### 4.3.4.2 Ist-Analyse

Die Ist-Analyse des derzeitigen Teilsystems ist in jedem Migrationsgebiet der erste notwendige Schritt; er sollte in diesem Fall damit beginnen, die Häufigkeitsverteilung der verwendeten Office-Pakete samt der jeweiligen Versionen zu bestimmen. Anhaltspunkte hierzu liefern Behörden-interne Richtlinien und mit Softwarelieferanten geschlossene Rahmenverträge, die allerdings beide nur den „Mainstream" abdecken; daher sollten hierzu auch Anwender aus verschiedenen Bereichen und mit unterschiedlichem Anforderungsprofil befragt werden. Dabei sollte zugleich ermittelt werden, ob lediglich die Basiskomponenten der jeweiligen Office-Suite zum Einsatz kommen oder weitere Komponenten für die tägliche Arbeit relevant sind. Für jede eingesetzte Komponente gilt es zudem, die jeweils benötigte Funktionalität festzustellen und auch, welche Funktionen Probleme bereiten oder derzeit gänzlich fehlen.

Hinsichtlich der Dateiformate ist für die Basiskomponenten zu klären, welche aktuellen Formate derzeit als Standard verwendet werden können (Formatunterstützung), welche älteren Dokumentenformate die aktuelle Office-Suite lesen und sinnvoll darstellen kann (Abwärtskompatibilität) und in welchen relevan-

[153] http://www.openoffice.org
[154] http://www.documentfoundation.org
[155] siehe http://www.muenchen.de/limux

ten Formaten neben dem eigenen Standard Dokumente geschrieben werden können (Exportfunktionalität).

Die über den Einsatz der Basiskomponenten hinausgehende Verwendung weiterer Office-Komponenten sollte näher betrachtet und die Anzahl und der Zweck von Eigenentwicklungen sogenannter aktiver Inhalte oder von Desktop-Datenbanken festgestellt werden (siehe Abschnitt 4.3.4.2.1). Schließlich ist die originäre Aufgabe einer Office-Suite der Umgang mit und der Austausch von elektronischen Dokumenten; eine darüber hinaus gehende Nutzung der Office-Suite kann zu unerwünschten Überschneidungen mit anderen Teilsystemen führen und auch Zuständigkeiten anderer Organisationseinheiten berühren.

#### 4.3.4.2.1 Stolperfallen

Eigenentwicklungen sogenannter aktiver Inhalte (Makros, Skripte) in Dokumenten und Vorlagen oder selbst erstellte Desktop-Datenbanken sind praktisch in jeder Behörde anzutreffen, teils entstanden als persönliche Arbeitserleichterung bei wiederkehrenden Aufgaben, teils als Umsetzung kurzfristig benötigter, aber nicht (oder nicht schnell genug) in der IT-Planung vorgesehener Funktionalitäten oder Datenbestände. Diese Eigenentwicklungen treten meist in mannigfacher Vielfalt ohne zentrale Koordinierung auf und sind zu Beginn einer Migration in der Regel weder erfasst noch im Umfang abschätzbar. Sie stellen ein erhebliches Risiko bei jeder Migration von Office-Suiten dar, weil deren jeweilige technologische Voraussetzungen und die Anzahl an Nutzern zumindest nicht im vollen Umfang bekannt sind. Folglich kann auch nicht abgeschätzt werden, wie viele Eigenentwicklungen überhaupt migriert werden und für welche Eigenentwicklungen künftig welche Voraussetzungen für deren weiteres Funktionieren existieren müssen. Dieselben Effekte können beim Einsatz von Erweiterungen (Plug-Ins) auftreten. Damit kann der Soll-Zustand nicht vollständig definiert werden, eine Fortführung der Migration wäre von vorn herein zum Scheitern verurteilt.

#### 4.3.4.2.2 Erfassung von Eigenentwicklungen und Erweiterungen

Es ist daher notwendig, im Rahmen der Ist-Analyse möglichst alle von Behördenbediensteten genutzte Eigenentwicklungen und Erweiterungen auf der Basis der derzeitigen Office-Komponenten zu erfassen, insbesondere

- Formulare und Tabellenkalkulationen mit Programmlogik (z.B. selbst entwickelte Feldvalidierung, Freischalten anderer Felder),
- VBA-Skripte und vergleichbare Kleinanwendungen,
- sonstige Makros in Dokumenten und Dokument-Vorlagen,
- Desktop-Datenbanken auf der Basis von Microsoft Access oder LibreOffice Base und
- eingesetzte Erweiterungen.

Da die Erfassung möglichst lückenlos sein soll, ist eine stichprobenweise Befragung von Anwendern unzureichend. Vielmehr sollten sämtliche Nutzer der derzeitigen Office-Suiten mindestens dahingehend Auskunft geben,

- welche Eigenentwicklungen und Erweiterungen sie einsetzen (Bezeichnung, verwendete Technik),
- in welcher Häufigkeit sie dies tun,
- welchen Zweck die jeweilige Eigenentwicklung oder Erweiterung hat (welche Arbeit wird erleichtert),
- welchen Grund es für die *Eigen*entwicklung gibt (z.B. fehlende Haushaltsmittel, Ablehnung durch IT-Abteilung),
- wie wichtig die jeweilige Eigenentwicklung oder Erweiterung für die Erledigung der täglichen Arbeiten ist (z.B. Zeitersparnis, keine adäquate Datenquelle verfügbar),

- welche Voraussetzungen für deren Funktionieren notwendig sind (z.B. Zugriff auf andere Eigenentwicklungen oder Erweiterungen wie Personen- oder Sachlisten) und
- wie viele andere Anwender diese Eigenentwicklung oder Erweiterung ebenfalls nutzen oder in sonstiger Form davon profitieren.

Diese Anwenderbefragung könnte zwar beispielsweise über eine Intranet-Onlinebefragung für die gesamte Behörde umgesetzt werden, doch ist kaum anzunehmen, dass alle Anwender daran teilnehmen, und auch die Qualität der Antworten dürfte eher durchwachsen sein. Sinnvoller ist es, den seit 2007 im Münchner LiMux-Projekt beschrittenen Weg zu gehen[156]. Dort hat sich gezeigt, dass die Aufteilung der Migration auf einzelne Abteilungen und der Einsatz von mindestens zehn Prozent an Pilot-Anwendern je Abteilung sehr hilfreich war, um „den Grad der Heterogenität der jeweils gewachsenen IT-Landschaften herauszufinden“ und die gröbsten Hürden für die Migration auch der übrigen Anwender festzustellen. In dieser Granularität ist es zudem möglich, die oben genannten Fragen zur Verwendung von Eigenentwicklungen und Erweiterungen durch Interviews beantworten zu lassen.

Die mit dem Projekt betrauten Migrations-Experten sind bei dieser Vorgehensweise schon sehr bald in der Lage, die richtigen Fragen zu stellen, um ein möglichst vollständiges Bild aller Migrationshemmnisse in Erfahrung zu bringen. Allerdings ist der Zeitaufwand bei dieser in München „Keimzellen-Strategie“ genannten Vorgehensweise enorm. Es ist daher sinnvoll, nach den ersten Erfahrungen einen Prozess mit den *Best Practices* aufzusetzen und diesen über Multiplikatoren parallelisiert anzuwenden.

#### 4.3.4.2.3 Konsolidierung der Erkenntnisse

Die festgestellten Eigenentwicklungen müssen abgeglichen werden, um gleiche oder ähnliche Lösungen erkennen und zusammenführen zu können. Auch gilt es herauszufinden, auf welchen Technologien die Eigenentwicklungen zu welchen Anteilen basieren. Schließlich sollten die solcherart konsolidierten Erkenntnisse für die anstehende Migration in ihrer Gesamtheit priorisiert werden, wobei die von den Anwendern vorgenommene Priorisierung zu berücksichtigen ist.

Spätestens jetzt wird deutlich, dass die Einrichtung eines entsprechend dimensionierten Projektbüros unumgänglich ist. Dieses sollte flankiert werden von einer mit den Migrationsthemen und -problemen vertrauten Anwenderunterstützung, die zugleich als „Eingangsfilter“ für die gemeldeten Eigenentwicklungen dienen kann.

#### 4.3.4.2.4 Ergebnis

Die Ist-Analyse kann beim Einsatz verschiedener Versionen einer Office-Suite und erst recht beim Einsatz verschiedener Office-Suiten in einer Behörde zu einer großen Bandbreite an weiterhin benötigter oder künftig geforderter Funktionalität führen. Eine Unterteilung der einzelnen Funktionen in eine Basisfunktionalität für den überwiegenden Einsatz und eine spezifische Funktionalität für wenige Einsatzgebiete ist daher sinnvoll; das Ergebnis sollte eine Liste von Mindest-Anforderungen an die Basisfunktionalität für die Soll-Konzeption sowie ggf. eine Liste mit weiteren, spezifischen Anforderungen an die künftige Office-Suite oder an andere Teilsysteme sein. Zudem sollten diese Anforderungen neben einer Bewertung des jeweiligen Nutzens analog zu den Eigenentwicklungen eine Priorisierung erfahren, um bei einer Migration zunächst die wesentlichen Aspekte umsetzen zu können, bevor Spezifika für Randgebiete in den Fokus rücken. Die endgültige Zuordnung der einzelnen Anforderung zum umsetzenden Teilsystem wird in der nächsten Migrationsphase, der Soll-Konzeption, festgelegt. Das bedeutet, dass die bei der Betrachtung der Office-Komponenten notierten Anforderungen nicht notwendigerweise auch in Zukunft mit Office-Mitteln umgesetzt werden müssen.

[156] siehe http://www.heise.de/ct/meldung/LiMux-Projektfuehrung-Wir-waren-naiv-958642.html

#### 4.3.4.3 Soll-Konzeption

Im Rahmen der Soll-Konzeption sind die künftig notwendigen Komponenten und Funktionalitäten für den Behördenbetrieb zu bestimmen, also die funktionalen Anforderungen an die künftige Office-Suite festzulegen. In den meisten Fällen dürften die Basiskomponenten zur Textverarbeitung, zur Tabellenkalkulation und zur Präsentation in ihrer Grundfunktionalität ausreichen. Aus der Ist-Analyse sollten die darüber hinausreichenden domänenspezifischen Anforderungen der Behörde hervorgehen. Diese gilt es kritisch dahingehend zu beleuchten, ob die weitergehenden Anforderungen

- durch vorhandene Funktionalitäten der Basiskomponenten in der künftigen Office-Suite bereits abgedeckt sind,
- vom Umfang und der Thematik her eher anderen Teilsystemen zuzuordnen und ggf. von diesen zu realisieren sind oder
- tatsächlich mittels zusätzlicher Office-Komponenten oder gar von Office-basierten Eigenentwicklungen abgedeckt werden müssen.

##### 4.3.4.3.1 Desktop-Datenbanken

Insbesondere der Einsatz von Desktop-Datenbanken wie Microsoft Access oder LibreOffice Base sollte künftig vermieden oder wenigstens stark zurückgefahren werden, weil einerseits ihre Dateiformate nicht standardisiert sind und daher auch künftige Migrationen erschweren, und weil andererseits die damit möglichen „persönlichen Datenbanken“ regelmäßig nicht von der IT-Abteilung erfasst sind. Damit sind weder die gesammelten Daten noch die programmierte Funktionalität einem größeren Kreis von Anwendern bekannt, eine Nutzung der Daten und der Funktionalität durch weitere Anwender wird verhindert; eine parallele Vollnutzung (Lese- und Schreibzugriffe) solcher Datenbanken scheidet aufgrund des dateibasierten Ansatzes der Datenhaltung ohnehin aus. Auch sind die Daten nicht in die regelmäßigen Sicherungsläufe des IT-Betriebs eingebunden und daher nicht ausreichend gegen Datenverlust gesichert. Da inhaltlich ähnliche Daten meist an mehreren Stellen benötigt werden, sind zudem Redundanzen wahrscheinlich. Der Redundanzverdacht gilt auch für die eigenentwickelten Funktionalitäten, die in ähnlicher Form bei vielen Desktop-Datenbanken aufkommen. Ingesamt überwiegen also beim Einsatz von Desktop-Datenbanken die Aspekte, die mit Risiken und unnötigen Kosten verbunden sind und nicht den Grundsätzen von Datensicherheit, -sparsamkeit und Wiederverwendung entsprechen.

Da es allerdings meist belastbare fachliche Gründe für die Nutzung der in Eigenregie erstellten Desktop-Datenbanken gibt, sollte jeweils geprüft werden, ob eine Übergabe des Datenbestands an die IT-Abteilung sinnvoll ist und dadurch Datenhaltung und -sicherung professionalisiert, die Bereitstellung von Funktionalität zentralisiert sowie der Zugriffs- und der Datenschutz den Behördenstandards angeglichen werden können. Der lesende Zugriff darauf ist für den bisherigen „Eigentümer“ der Desktop-Datenbank weiterhin mit Office-Mitteln möglich, allerdings müssen für die Datenpflege geeignete Werkzeuge bereitgestellt werden. Dies kann sich insbesondere bei komplexeren Datenstrukturen zu einem eigenständigen Realisierungsprojekt auswachsen, aber bei einer entsprechend hohen Anwenderzahl trotzdem wirtschaftlich sein.

##### 4.3.4.3.2 Aktive Inhalte

Auch die sogenannten aktiven Inhalte sind nicht standardisiert. Daher gilt für sie grundsätzlich dasselbe wie für die Desktop-Datenbanken. Zwar können innerhalb derselben Produkt-Familie die meisten Makros und Skripte automatisiert übernommen werden, doch lassen sich Probleme bei komplexen oder verschachtelten Konstrukten nicht grundsätzlich ausschließen. Soll die Produkt-Familie oder das Standard-Dokumentenformat gewechselt werden, ist eine automatisierte Übernahme regelmäßig nicht möglich, die aktiven Inhalte müssen in der neuen Office-Suite neu erstellt werden. Dadurch kann erheblicher Aufwand entstehen und sollte ebenfalls als eigenständiges Realisierungsprojekt betrachtet werden. Sinnvoll ist auch hier eine zentrale Bereitstellung der bisher in Eigenregie erstellten und vorgehaltenen

Vorlagen und Formulare, damit ein möglichst großer Anwenderkreis davon profitieren kann. Bei der Umsetzung dieses Gedankens hilft erneut ein Blick nach München – die Stadt hat für dieses Thema ein eigenständiges Open-Source-Projekt namens WollMux[157] initiiert und 2008 unter der European Union Public Licence (EUPL) freigegeben. Die Resultate können damit u.a. von jeder Behörde genutzt und ggf. erweitert werden.

#### 4.3.4.3.3 Basisfunktionalität

Sind die Eigenentwicklungen und Erweiterungen separiert, wird der Blick frei für die Migration der Basiskomponenten. Deren jeweilige künftige Basisfunktionalität sollte mindestens den Forderungskatalog der Ist-Analyse umfassen (siehe Abschnitt 4.3.4.2.4). Die Leistungsfähigkeit aktueller Basiskomponenten ist umfassend, die aus der Sicht des Migrationsleitfadens wichtigsten können den Bewertungen einzelner Funktionalitäten entnommen werden (siehe Tabellen in Abschnitt 4.3.4.5).

#### 4.3.4.3.4 Dokumentenformate

Für den Datenaustausch geben der SAGA-Standard (Die11b) und der in der Einleitung genannte ODF-Beschluss den Rahmen für die zu verwendenden Dokumentenformate vor. Gemäß Ersterem ist zwischen Formaten zum Informationsaustausch und zur Weiterbearbeitung zu unterscheiden. Als Informationsaustausch wird das originalgetreue Bereitstellen von Informationen ohne Weiterverarbeitung bezeichnet. SAGA schreibt hierfür verbindlich das Portable Document Format (PDF) ab der Version 1.4 vor. Dies gilt gleichermaßen für Textdokumente, Tabellenkalkulationen und Präsentationen und für alle Arten von Empfängern. Außerdem empfiehlt SAGA für Tabellen und Präsentationen zusätzlich die Bereitstellung im Format HTML 4.01. Damit ist bei der Evaluierung der Office-Suiten zu prüfen, ob derartige Dokumente aus der Office-Suite heraus erstellt werden können. Das Lesen von PDF-Dokumenten hingegen ist keine Anforderung an Office-Suiten und wird in einem eigenen Abschnitt behandelt (siehe 4.3.7); gleiches gilt für HTML-Dokumente, die mit Browsern gelesen werden (siehe 4.3.2).

Gemäß dem ODF-Beschluss müssen die Probanden zudem mit ODF-Dokumenten so umgehen können, dass deren Erstellen und Bearbeiten gewährleistet ist und ODF-Dokumente *empfangen* werden können, was sinngemäß das standardkonforme Lesen und Darstellen deren Inhalte bedeutet. Gemäß SAGA gilt dies für Dokumente, die zur Weiterverarbeitung bestimmt sind. Der ODF-Beschluss verweist auf die entsprechende Norm ISO/IEC 26300:2006, die das OASIS Open Document Format for Office Applications (ODF) in der Version 1.0 beschreibt. Allerdings ist die Normierung von ODF v1.1 als *Amendment* (Novellierung) zu ODF v1.0 derzeit in Arbeit. SAGA führt folglich ODF v1.0 als „Bestandsgeschützt“ und die Version 1.1 als „Beobachtet“. ODF v1.2 ist von der zuständigen OASIS-Arbeitsgruppe[158] am 26.03.2011 verabschiedet und von den Mitgliedern des OASIS International Standards Consortiums am 05.10.2011 als offizieller OASIS-Standard angenommen worden[159], wird in SAGA allerdings noch nicht aufgeführt. ODF v1.2 bringt gegenüber Version 1.1 neben den üblichen Korrekturen einige Verbesserungen, insbesondere

- Openformula zum Austausch von Formeldefinitionen zwischen verschiedenen Anwendungen,
- die Aufnahme von RDF-Metadaten zur Einbeziehung von W3C-Standards wie vCards oder Caldav sowie
- die Unterstützung für digitale Signaturen.

Im Abschnitt „Hintergrund“ des ODF-Beschlusses wird außerdem angeführt, dass „die Bundesverwaltung [...] in der Lage sein [muss], zunächst weiterhin diese elektronischen Dokumente [gemeint sind die bisherigen Binärformate der Microsoft Office Software-Suite] mit ihren Partnern und Kunden auszutauschen und gemeinsam zu bearbeiten“. Entsprechend sind diese in SAGA als „Bestandsgeschützt“

[157] http://www.wollmux.org
[158] OASIS Open Document Format for Office Applications (OpenDocument) TC
[159] Siehe Pressemittelung unter http://www.oasis-open.org/news/pr/odf-1-2-approval

aufgeführt. Die von Microsoft entwickelten Office Open XML File Formats (OOXML) stehen in beiden Dokumenten unter dem Vorbehalt der Beobachtung, in SAGA zudem unterschieden nach „Transitional“ und „Strict“.

Insgesamt ergibt sich also ein heterogenes Bild für die Formate der zur Weiterbearbeitung bestimmten Dokumente. Zudem treffen weder SAGA noch der ODF-Beschluss eine Aussage darüber, in welchem Format Anwender ihre Dateien zu erstellen oder nach deren Bearbeitung zu speichern haben, solange kein Datenaustausch stattfindet. Daraus kann allerdings nicht auf eine diesbezüglich freie Wahl des Standard-Dokumentenformats geschlossen werden. Vielmehr gilt es, die Intention dieser für die Bundesverwaltung verbindlichen Dokumente zu berücksichtigen. Deren Tenor ist die „Förderung offener Dokumentenaustauschformate“, insbesondere von ODF, die bisherigen Microsoft-Binärformate sollen nur übergangsweise zur Abwärtskompatibilität unterstützt werden. Das von Microsoft Office 2010 verwendete Format OOXML Transitional hat zudem den Nachteil, dass dessen Anteile zur Unterstützung älterer Versionen der Microsoft Office Suite „für Dritte nur schwer zu implementieren sind“[160] und dass Microsoft Office den Standard selbst nicht vollständig einhält, was man den von Microsoft veröffentlichten umfangreichen „Implementer's notes'"[161] entnehmen kann. Die Verwendung von ODF ist daher vorzuziehen.

Damit muss die Office-Suite sicher mit ODF-Dokumenten und den Binärformaten früherer Microsoft-Office-Versionen zurechtkommen, die Unterstützung sonstiger Dateiformate ist für die allgemeine Bewertung nicht relevant. Letztere sollten allerdings je Behörde anhand der Ist-Analyse mit den derzeit vorhandenen Datenbeständen und deren Formaten abgeglichen werden. Pluspunkte gibt es, sofern einzelne ODF-Versionen für das Dokumentenformat ausgewählt werden können, Abzüge hingegen für Verletzungen der Konformität zum Standard.

Das beim Arbeiten mit Office-Suiten verwendete Dokumentenformat sollte Behörden-weit eindeutig vorgegeben und bei der Installation des Produkts entsprechend eingerichtet werden können, um potentielle Schwierigkeiten im internen Arbeitsumfeld und in mit der Dokumentbearbeitung verbundenen Prozessen und Systemen zu minimieren.

#### 4.3.4.4 Betrachtete Alternativen

Eine empirisch fundierte Produktauswahl anhand der tatsächlichen Verbreitung ist im Kontext der Office-Suiten nicht möglich. Weder existieren hierzu repräsentative Umfragen, noch eignen sich dazu allein die Verkaufszahlen einzelner Hersteller, weil Open-Source-Lösungen frei zur Verfügung stehen und dabei unbeachtet blieben. Somit werden aufgrund von Schätzungen folgende Produkte in der jeweils aktuellen Version betrachtet:

- **Microsoft Office** als die in Behörden am häufigsten verwendete Lösung sowie
- **LibreOffice** als die am weitesten verbreitete Office-Suite im Open-Source-Umfeld.

Auf einen weiteren lokal zu installierenden Probanden wird mangels derzeitiger Relevanz verzichtet. Ebenfalls nicht betrachtet werden sogenannte Public-Cloud-Offices, bei denen Funktionalitäten einer Office-Suite in mehr oder weniger ausgeprägter Form von Wirtschaftsunternehmen gegen Gebühr über das Internet angeboten werden. Zwar hat eine solche Lösung den Charme, dass keine lokale Installation auf dem Arbeitsplatzrechner des Anwenders notwendig ist, doch fehlt es derzeit sowohl an klaren und verbindlichen Sicherheitsstandards als auch angesichts der Ortstransparenz von Public-Clouds an Rechtssicherheit, insbesondere hinsichtlich des Datenschutzes (Wei10).

#### 4.3.4.5 Bewertung

Die nachfolgende Bewertung der Probanden basiert auf möglichst allgemeingültigen Kriterien und kann weiter verfeinert, erweitert oder anders gewichtet werden. Geprüft werden unter anderem die Auswahl-

[160] siehe (Die11b) unter 7.2.2 zu „Beobachtet: Office Open XML (OOXML)/ISO/IEC 29500 Strict“
[161] http://msdn.microsoft.com/en-us/library/gg696065.aspx

möglichkeit der Komponenten, deren Basisfunktionalität, der jeweilige Umgang mit Dokumentenformaten und die jeweilige Kompatibilität zum ODF, möglichst getrennt nach dessen Versionen.

#### 4.3.4.5.1 Komponenten und Installation

Im Rahmen des Migrationsleitfadens werden Textverarbeitungs-, Tabellenkalkulations- und Präsentationsmodule als Basiskomponenten betrachtet. Alle Microsoft Office 2010 Editionen enthalten die betrachteten Basiskomponenten, so auch die für Behörden meist relevante Microsoft Office Professional Plus 2010. LibreOffice enthält alle betrachteten Basiskomponenten.

Sonstige Komponenten der Office-Pakete sollten gezielt hinzugezogen oder abgewählt, die gewünschte Auswahl für eine Vielzahl von Installationen zentral definiert und die Installationsquelle für alle Arbeitsplatzrechner zentral bereitgestellt werden können. Diese Möglichkeiten bieten beide Office-Suiten, sie unterscheiden sich lediglich dahingehend, dass Microsoft bei Volumenlizenzen ein eigenes *Office Customization Tool* zur Bearbeitung von Installationseinstellungen mitliefert, während LibreOffice kein entsprechendes Werkzeug beiliegt. Damit können beide Probanden mittels Werkzeugen zur Softwareverteilung (siehe Kapitel 4.2.6 Client-Management auf Seite 105) für eine Vielzahl von Arbeitsplatzrechnern zentral verwaltet werden, die jeweilige Dokumentation findet sich für Microsoft Office in (Mic10a) und für LibreOffice in (Ope11).

Tabelle 4.11: Vergleich Verfügbarkeit und Installation

| **Office-Suite** | **Microsoft Office 2010** | **LibreOffice 3.4** |
|---|---|---|
| **Metainformationen** | | |
| Lizenz | Proprietär | OSS |
| Unterstützte Plattformen<br>Windows XP / Windows 7 / Linux / MacOS X | ✓/✓/–/✓[162] | ✓/✓/✓/✓ |
| **Installation** | | |
| Behördenweite Installationsvorgaben | ✓ | ✓ |
| Zentrale Installationsquelle | ✓ | ✓ |
| Auswahl von Komponenten | ✓ | ✓ |
| Standard-Dokumentenformat ODF | ✓[163] | ✓ |

#### 4.3.4.5.2 Grafische Benutzerschnittstelle

LibreOffice verwendet die sogenannte klassische Benutzersteuerung mit einer Menüzeile und verschiedenen zu- und abwählbaren Symbolleisten. Diese grafischen Steuerungselemente werden in ähnlicher Form von den meisten Anwendungen des Bürobereichs verwendet, sind ein etablierter Software-Standard und stellen eine gewohnte Form des Umgangs mit Software-Produkten für die meisten Anwender dar.

Microsoft Office hat mit der Version 2007 eine neue Benutzersteuerung namens *Ribbons* eingeführt, die thematisch ähnliche Funktionen jeweils auf einer breiten Multifunktionsleiste gruppiert und dafür auf zu- oder abwählbare Symbolleisten ebenso verzichtet wie auf die übliche Menüstruktur. Die Sortierung der Elemente weicht teils stark von der Menüstruktur der Vorgänger ab und erfordert eine entsprechende Einarbeitung der Anwender. Eine Rückkehr zur früheren Bedienlogik mit Menüzeile und Symbolleisten ist nicht möglich.

[162] Für Mac OS X bietet Microsoft eine eigene Office-Suite an.
[163] ODF kann bei der Installation anstelle von OOXML als Standard-Dokumentenformat vorgegeben werden.

Bei einer Migration von Microsoft Office-Versionen vor 2007 oder von sonstigen Office-Suiten zu Microsoft Office 2010 sollte daher berücksichtigt werden, dass alle Anwender unter anderem im Umgang mit der neuen Benutzerschnittstelle geschult werden müssen.

#### 4.3.4.5.3 Dokumentenformate

LibreOffice verwendet per Voreinstellung das OASIS Open Document Format for Office Applications (ODF) in der Version 1.2, Microsoft Office den eigenen Standard Office Open XML File Formats (OOXML) in der Variante *transitional conformance*, welche der Abwärtskompatibilität zu früheren Microsoft-Formaten dient[164]; beispielsweise kann eine von der strikten Variante abweichende Darstellung von Leerräumen nach Art von Word 95 erzwungen werden.

Bei beiden Office-Suiten ist eine Umstellung auf ein anderes Standard-Dokumentenformat möglich. Microsoft Office kann auf „ODF“ umgestellt werden und verwendet dann dessen Version 1.1. LibreOffice kann auf „ODF 1.0 / 1.1“ als Standard-Dokumentenformat umgestellt werden; angesichts der gegenüber der Vorversion deutlichen Verbesserungen und der Kompatibilität zu Version 1.1 ist dies aber prinzipiell nicht notwendig. Beide Office-Suiten sprechen Warnungen vor Formatierungs- und sonstigen Verlusten aus, wenn nicht im jeweils ursprünglichen Dokumentenformat gespeichert wird, und verweisen auf teils sehr detaillierte Listen mit nicht, teilweise oder vollständig unterstützten Formateigenschaften, beispielsweise (Mic10b). Bei der Betrachtung der einzelnen Komponenten wird hierauf näher eingegangen.

ODF-Dokumente können mit dem Open-Source-Werkzeug ODF Validator[165] auf syntaktische Korrektheit gegenüber dem ODF-Standard geprüft werden. Zur Auswahl stehen hierbei die ODF-Versionen 1.0, 1.1 und 1.2 und verschieden strenge Prüfläufe. Office-o-tron[166] bietet als weiteres Open-Source-Werkzeug zudem die Prüfung von OOXML-Dokumenten an, stellt aber derzeit[167] deutlich weniger Mängel bei den ODF-Testdateien (s.u.) fest als der ODF Validator. Mit OfficeShots[168] steht ein weiteres Prüfwerkzeug zur Verfügung, welches die Verwendung von ODF Validator und Office-o-tron mit einer variablen Menge von Office-Applikationen kombiniert und verschiedene Prüfläufe anbietet (z.B. PDF-Erstellung, Roundtrip). Damit ist beispielsweise eine manuelle Semantik-Prüfung anhand der im Prüflauf erstellten Dokumente möglich.

Allerdings weisen alle genannten Werkzeuge darauf hin, dass deren Prüfergebnisse lediglich Anhaltspunkte für eingehendere Prüfungen darstellen und nicht verbindlich sind. Ein verbindliches Prüfinstrument wird weder von OASIS noch sonstigen Normierungsgremien oder Behörden bereitgestellt. Das OASIS Open Document Format Interoperability and Conformance (OIC) Technical Committee[169] ist beauftragt, Methoden und Hilfsmittel (z.B. Prüfprofile, Testdokumente) zur Konformitäts- und Interoperabilitätsprüfung zu erstellen, wird allerdings weder Produkt-Zertifizierungen durchführen noch Software er- oder bereitstellen, mit der Konformität oder Interoperabilität getestet werden kann. Der Ende 2010 erstellte Report zur Interoperabilität der verschiedenen ODF-unterstützenden Produkte verweist darauf, dass die syntaktische Einhaltung des Standards noch keine Aussage über die Interoperabilität zulasse, allerdings eine wesentliche Voraussetzung dafür sei (OAS10). Immerhin enthält er eine Liste von Qualitätsmerkmalen, auf die hinsichtlich der Interoperabilität von Office-Dokumenten zu achten ist:

1. Die übereinstimmende grafische Repräsentation des Dokuments in verschiedener Hinsicht, u.a. Schriftsatz und -größe, Zeilenabstand, Darstellung von Umlauten u.ä., Durchschuss, Seitenumbrüche.

2. Der Erhalt der Dokumentstruktur, insbesondere Überschriften, Absätze, Listen und Tabellen.

[164] „provide support for legacy Microsoft Office applications“, „features for backward-compatibility and that are useful for high-quality migration of existing binary documents to ISO/IEC 29500“
[165] http://tools.services.openoffice.org/odfvalidator/, Stand 08.06.2011 in Version 1.0
[166] http://www.probatron.org:8080/officeotron/officeotron.html
[167] Stand 07.06.2011 in Version 0.6.3
[168] http://www.officeshots.org/
[169] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=oic

3. Das korrekte Verhalten von Querverweisen und externen Referenzen.
4. Das gleichartige Verhalten und die gleichartige Darstellung von eingebetteten Bildern, Medien und sonstigen Objekten.
5. Der Erhalt der Metadaten des Dokuments.
6. Der Erhalt von Dokument-Erweiterungen, z.B. Zeichnungen.
7. Die Integrität von digitalen Signaturen und sonstigen Schutzmechanismen.
8. Das gleichartige Laufzeitverhalten aktiver Inhalte wie Skripte und Makros.

Diese Qualitätsmerkmale sollten für die jeweilige Behörde hinsichtlich ihrer Relevanz für übliche Dokumentinhalte gewichtet und deren Einhaltung durch Tests mit verschiedenen repräsentativen Dokumenten geprüft werden. Dazu sollten sowohl manuelle als auch automatisierte Konvertierungen vom derzeitigen in das künftige Standard-Dokumentenformat vorgenommen und anhand der bisherigen und der künftigen Office-Suite der Grad der Interoperabilität ermittelt werden. Die Möglichkeiten zur Konvertierung bestehender Dokumente von Microsoft-Formaten in ODF können dem Praxishandbuch zum ODF-Beschluss (Bun11) entnommen werden, welches die Bundesstelle für Informationstechnik (BIT) Behörden auf Nachfrage zur Verfügung stellt.

#### 4.3.4.5.4 Textverarbeitung

Die Textverarbeitung ist die von Behörden meistverwendete Komponente einer Office-Suite, mit ihr wird die überwiegende Mehrzahl an Dokumenten erstellt. Bei einer Migration sollte ihr daher auch die größte Aufmerksamkeit gewidmet werden.

**Microsoft Word 2010** zeigt bei der Untersuchung der Basisfunktionalität kleine Schwächen. Konkret funktioniert die maschinelle Feldzuweisung bei der automatischen Dokumentenerstellung nicht voll zufriedenstellend[170]. Beim Etikettendruck führt der Austausch einer Formatvorlage zum Verlust aller bisherigen Feldzuordnungen. Beim Importieren und Darstellen unterschiedlicher Medientypen ergeben sich bei Word 2010 hingegen keinerlei Probleme – das Einfügen, Verschieben, Vergrößern und Verkleinern von Bildern und Grafiken (Grafikformat der Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF), Portable Network Graphics (PNG) und Scalable Vector Graphics (SVG)) klappt anstandslos. Umfangreiche Dokumente handhabt der Microsoft-Proband sowohl bei der automatischen Dokumentenerstellung als auch bei der normalen Textverarbeitung (B$^+$10) einwandfrei. Das Einfügen und Verwalten von Diagrammen und Tabellen funktioniert ebenfalls problemlos. Positiv fallen hier die zahlreichen Einstellungsmöglichkeiten bzgl. des Aussehens der Diagramme auf. Die obligatorische Rechtschreibprüfung ist vorhanden, hat allerdings einige kleinere Probleme (B$^+$10).

Bei der Formatunterstützung zeigt Word 2010 Probleme beim testweisen Öffnen des Migrationsleitfadens 3.0 als ODF (Version 1.1). Beispielsweise werden das Inhaltsverzeichnis falsch formatiert, Teile des Textes fälschlicherweise fettgedruckt und die einzelnen Kapitel anders durchnummeriert als im Inhaltsverzeichnis. Dieses passt sich erst nach einer Aktualisierung an, dabei werden allerdings unterschiedliche Gliederungsebenen fälschlich gleichbehandelt. Auch beim Bearbeiten der Datei zeigt der Microsoft-Proband einige Probleme; es ist zum Beispiel nicht möglich, die Daten eines eingebetteten Diagramms zu verändern. Bei der Serienbrieferstellung kann eine OpenDocument Spreadsheet (ODS)-Tabelle nicht als Adressenquelle verwendet werden.

Microsoft hat eine Liste mit detaillierten Informationen zu Differenzen und Gemeinsamkeiten der Formatfamilien ODF und OOXML hinsichtlich der Textverarbeitung bereitgestellt (Mic10e). Integrative Aspekte wie die Einbettung von Objekten und die Anbindung an externe Datenquellen gehen demnach ebenso verloren wie manche Formatierungen und Felder, aktive Inhalte, Abbildungsverzeichnisse und diverse

[170] Spalte in Excel-Arbeitsblatt mit Namen „Adresse“ wurde in Serienbrief-Dokument Feld „Adresse 1“ zugeordnet.

weitere Eigenschaften. Die fehlende Unterstützung der Änderungsverfolgung erschwert ein gemeinsames Bearbeiten von Dokumenten auf der Basis von ODF mit Microsoft Word deutlich. Insgesamt erlaubt die Kombination von Microsoft Word und ODF nur die Verarbeitung von Dokumenten mit relativ einfach strukturierten Inhalten. Dies bestätigt eine Studie des Fraunhofer-Instituts für Offene Kommunikationssysteme FOKUS (EZI09) über die Kompatibilität der beiden Formatfamilien.

Zur Überprüfung der Konformität von Microsoft Word 2010 zum ODF-Standard wurde beispielhaft ein Test durchgeführt. Ein mit Word erstelltes Testdokument mit Titel, Untertitel, verschiedenen Überschriften der Ebenen 1, 2 und 3 sowie einem Inhaltsverzeichnis wurden im Format OpenDocument Text (ODT) gespeichert und anschließend mit dem ODF Validator auf Korrektheit gegenüber dem entsprechenden XML-Schema geprüft. Je nach Rigidität des Prüfverfahrens (Auswahlfeld „test mode“) ergaben sich für ODF v1.1 stets mindestens zwei Fehler [171], in der „strict validation“ deren drei[172]. Für ODF v1.0 ergaben sich jeweils mindestens sechs Fehler [173], in der „strict validation“ deren sieben[174]. Prüft man hingegen mit Office-o-tron, werden keine Validitäts-Fehler gemeldet. Ob von Microsoft Word 2010 erstellte ODT-Dateien zu ODF v1.0 und v1.1 konform sind, ist mit diesen Hilfsmitteln folglich nicht zweifelsfrei zu ermitteln.

SUN XML Writer (SXW)-Dateien früherer OpenOffce-Versionen können mit Word 2010 nicht geöffnet werden. Dafür funktioniert das Öffnen und Bearbeiten von Microsoft Office Word Binärformat (DOC)- und Rich Text Format (RTF)-Dateien problemlos. Auch Word 2007-Dateien mit Tabellen, diversen Verzeichnissen, Bildern und Grafiken können einwandfrei geöffnet und bearbeitet werden. Insgesamt liegt eine auf die Microsoft-eigenen Formate eingeschränkte Abwärtskompatibilität vor.

Der Export einer Datei in das DOC-Format funktioniert großteils ($B^+10$) problemlos. Hierbei führt Word 2010 eine Kompatibilitätsprüfung durch und warnt vor Exportproblemen. Diese entstehen bei der Verwendung neuer Funktionen, die in älteren Word-Versionen nicht zur Verfügung stehen, und äußern sich beispielsweise darin, dass Formeln in Bilder umgewandelt werden oder Tabelleninhalte, die einen gewissen Umfang übersteigen, verloren gehen. Gleiches gilt für den Export in das RTF. Speichert man das Testdokument als ODF 1.1 und öffnet es mit LibreOffice, befinden sich u.a. einige Bilder nicht an den definierten Plätzen. Ein Export nach SXW wird gar nicht angeboten. Bei der HTML-Erstellung inkl. Hyperlinks, diverser Tabellen und Grafiken entstehen keine sichtbaren Fehler. Gleiches gilt für den Export in PDF. Ein Export in eine reine Textdatei wird ebenfalls angeboten.

**LibreOffice Writer** [175] zeigt bei der Basisfunktionalität ebenfalls leichte Schwächen. Wie MS Word bietet auch der LibreOffice Writer je einen Assistenten zur Erstellung von Serienbriefen und Etiketten, die beide ein einfaches Erstellen derartiger Dokumente ermöglichen. Nicht vorhanden ist ein Assistent zur Erstellung von Briefumschlägen – dies muss entweder über den Etiketten- oder den Serienbriefdruck realisiert werden.

Medientypen wie JPEG, GIF, PNG und SVG können problemlos eingefügt und bearbeitet werden. Umfangreiche Dokumente handhabt der Open-Source-Proband genauso problemlos ($B^+10$) wie das Erstellen und Bearbeiten von Diagrammen. Hier bietet der Writer zahlreiche Design-Vorlagen und Formatierungsmöglichkeiten. Das Einfügen, Gestalten und Formatieren von einfachen und umfangreichen Tabellen ist bequem und zügig möglich.

Die mitgelieferte Rechtschreibprüfung hat vor allem bei der Komposita-Bildung Probleme. Sie erkennt z.B. „Sortierfunktionen“ nicht und bietet „Tortierfunktionen“ als Alternative an. Sie kann allerdings durch eine andere Rechtschreibprüfung ergänzt oder ganz ersetzt werden, beispielsweise durch den Duden

[171] Die in META-INF/manifest.xml aufgeführten Dateien META-INF/manifest.xml und mimetype dürfen dort nicht enthalten sein. Die Begründung dafür findet sich allerdings erst in ODF 1.2 Part 3, Kap. 3.2.
[172] Zusätzlich zu den fehlerhaft aufgeführten Dateien wird das „unexpected attribute meta:non-whitespace-character-count“ moniert.
[173] Die für ODF v1.1 bemängelten fehlerhaften Dateieinträge, das „unexpected attribute text:use-soft-page-breaks“ sowie drei Mal „tag name text:soft-page-break is not allowed.“
[174] Zusätzlich zu den o.g. sechs Fehlern wird „unexpected attribute meta:non-whitespace-character-count“ bemängelt.
[175] Geprüft wurde Version 3.4

Korrektor[176]. Eine Grammatikprüfung wird zwar nicht mitgeliefert, kann aber ebenfalls nachgerüstet werden, z.B. durch den o.g. Duden Korrektor oder das quelloffene LanguageTool[177].

Hinsichtlich der Formatunterstützung überzeugt der LibreOffice Writer mit einer fehlerfreien[178] Unterstützung von ODF v1.2 für alle Prüftiefen. Wird er auf „ODF 1.0 / 1.1“ umgestellt, ergeben sich für die Conformance- und Validation-Prüfung gegen ODF v1.1 keine Fehler, die Strict Validation bemängelt allerdings deren zwei[179]. Die Prüfung gegen ODF v1.0 ergibt für Conformance und Validation drei Fehler[180], für die Strict Validation deren fünf[181]. Damit ist laut ODF Validator die Konformität des LibreOffice Writer zu ODF v1.0 ebenso fraglich wie bei MS Word, zu ODF 1.1 nahezu und zu ODF 1.2 vollständig gegeben. Dieselben Dateien, getestet mit Office-o-tron, ergeben hingegen in allen Testvarianten keine Validitätsfehler.

OOXML wird zwar in SAGA im Status „Beobachtet“ für änderbare Dokumentformate aufgeführt, aber nur für den Fall, dass „die Kompatibilität zu alten oder neuen Microsoft-Office-Versionen wichtig ist“[182]. Die Unterstützung von OOXML durch LibreOffice ist daher optional und für die allgemeine Bewertung nicht relevant. Ein kurzer Test ergab, dass der Writer Dokumente im entsprechenden Office Open XML Text (DOCX)-Format grundsätzlich lesen und einfache Dokumente korrekt darstellen kann. Auch kann er grundsätzlich Dateien im DOCX-Format speichern. Beim Öffnen eines so erstellten DOCX-Dokuments mit Word 2010 müssen allerdings gravierende Unterschiede festgestellt werden; neben Formatierungs-Differenzen geht in manchen Fällen auch Inhalt verloren[183]. Das gemeinsame Bearbeiten von DOCX-Dokumenten mit Word 2010 und dem LibreOffice Writer ist daher nicht zu empfehlen.

Hinsichtlich der Abwärtskompatibilität unterstützt der Writer Dokumente in den Formaten SXW und RTF vollständig, das DOC-Format weitgehend[184]. Mit MS Word 2007 erstellte Dateien führen hingegen in manchen Fällen zum Absturz des Writers. Insgesamt beschränkt sich die Abwärtskompatibilität des Writer nicht auf die eigenen früheren Formate, sondern umfasst auch weitgehend die der Microsoft Office Suiten.

Zum Exportieren von Dokumenten bietet der LibreOffice Writer neben den o.g. Möglichkeiten alle in SAGA oder dem ODF-Beschluss genannten Optionen. Dokumente können in den Formaten PDF, HTML, DOC, RTF und SXW gespeichert werden und entsprechen den jeweiligen Vorgaben. Auch ein Export in das in SAGA beobachtete DocBook-Format oder das dort empfohlene reine Textformat ist möglich.

Tabelle 4.12: Vergleich Textverarbeitung

| **Office-Komponente** | **MS Word 2010** | **LO Writer 3.4** |
|---|---|---|
| **Basisfunktionalität** | | |
| Medienunterstützung | ✓ | ✓ |
| Support großer Dokumente | ✓ | ✓ |
| Aufteilung in Kind-Dokumente | ✓ | ✓ |
| Einfügen/Verwalten von Diagrammen | ✓ | ✓ |
| Einfügen/Verwalten von Tabellen | ✓ | ✓ |

[176] http://www.duden-downloadshop.de
[177] http://www.languagetool.org/
[178] Getestet wurde eine zum Word-Test inhaltlich identische Datei mittels des ODF Validators.
[179] „unexpected attribute meta:non-whitespace-character-count“ und „unexpected attribute style:editable“
[180] „unexpected attribute text:use-soft-page-breaks“, 2x „tag name text:soft-page-breakïs not allowed“
[181] Wie Conformance, zusätzlich „unexpected attribute style:editable“, „unexpected attribute meta:non-whitespace-character-count“
[182] Siehe (Die11b) unter 7.7.2 zu „Beobachtet: Office Open XML (OOXML)/ISO/IEC 29500 Transitional“
[183] Z.B. fehlen sämtliche indizierten Worte im Text und werden nur im Index selbst aufgeführt.
[184] Beim Lesen von DOC-Dateien kann es bei Bildern und Grafiken zu geringfügigen Verschiebungen kommen.

| Office-Komponente | MS Word 2010 | LO Writer 3.4 |
|---|---|---|
| Rechtschreib- und Grammatikprüfung | ✓ | ✓[185] |
| Kommentare | ✓ | ✓ |
| Änderungsverfolgung | ✓ | ✓ |
| Einbinden externer Datenquellen | ✓ | ✓ |
| Dokumente vergleichen/zusammenführen | ✓/✓ | ✓/✓ |
| Einfügen/Verwalten von Verzeichnissen (Inhalt/Index/Tabellen/Abbildungen/Literatur/Rechtsgrundlagen) | ✓/✓/✓/✓/✓/✓/✓ | ✓/✓/✓/✓/✓/✓/- |
| Automatische Dokumenterstellung (Serienbrief/ Etiketten/ Umschläge) | ✓/✓/✓ | ✓/✓/✓[186] |
| **Formatunterstützung** | | |
| ODF v1.0 | - | - |
| ODF v1.1 | ✓[187] | ✓ |
| ODF v1.2 | - | ✓ |
| **Abwärtskompatibilität** | | |
| DOC | ✓ | ✓ |
| Word 2007 XML (Quasi-DOCX) | ✓ | ✓[188] |
| RTF | ✓ | ✓ |
| SXW | - | ✓ |
| **Exportfunktion** | | |
| PDF / PDF/A | ✓/✓ | ✓/✓ |
| Text | ✓ | ✓ |
| DocBook | - | ✓ |
| HTML 4.01 | ✓ | ✓ |

#### 4.3.4.5.5 Tabellenkalkulation

**Microsoft Excel 2010** weist eine breite Medientypenunterstützung auf und zeigt keine Probleme beim Einfügen, Vergrößern, Verkleinern und Zuschneiden von JPEG, GIF, PNG und SVG. Beim automatischen Fortführen von Zelleninhalten funktioniert das einfache Numerieren problemlos. Dabei sind auch Zahlenschritte größer eins möglich. Verwendet man Buchstaben statt Zahlen, kopiert Excel die markierten Zelleninhalte. Kombiniert man Zahlen und Buchstaben, funktioniert die Nummerierung nur, wenn die Zahl am Anfang steht oder durch ein Leerzeichen getrennt am Anfang bzw. Ende des Textes steht. Formeln werden mit automatisch angepassten Zellreferenzen weitergeführt.

In Tabellen kann nach Werten, Formeln und Kommentaren und dadurch in derselben Zelle entweder nach der zugrunde liegenden Formel, dem Ergebnis der Formel oder dem assoziierten Kommentar gesucht werden. Daten können vollständig oder in gewählten Teilbereichen nach vielfältigen Kriterien

[185] Über Plug-In
[186] Über Etiketten- oder Serienbriefdruck
[187] Laut ODF Validator wird ODF v1.1 von Word 2010 nicht korrekt umgesetzt, siehe Seite 138.
[188] Teilweise Abstürze, geringe Interoperabilität

auf- und absteigend sortiert werden. Eine Kombination verschiedener Sortierkriterien ist möglich. Zudem können Tabellen mit (Auto-)Filtern versehen werden, die nur die zutreffenden Datensätze anzeigen.

Excel bietet zahlreiche vorgefertigte Rechenfunktionen (Formeln), einen Assistenten zum Anwenden von Formeln sowie einen Formel-Debugger, der ein schrittweises Analysieren von Formeln zulässt (B+10). Zur Datenanalyse stehen u.a. Pivotfunktionen zur Verfügung, die Anbindung externer Datenquellen ist wie bei Word über ODBC und OLE DB möglich. Umfangreiche Dokumente mit mehreren tausend Zeilen können gelesen und gespeichert sowie Diagramme in vielfältiger Form eingefügt und verwaltet werden.

Mit Excel können Dateien im ODS-Format gelesen und gespeichert werden. Allerdings treten hier analog zu Word die Unterschiede zwischen den Office-Suiten und deren jeweiligen Standard-Dateiformaten zutage. Für herkömmliche Diagramme, Tabellen, Grafiken, Bilder und Formeln ist ein Datenaustausch auf ODS-Basis zwischen den verschiedenen Office-Suiten inhaltlich möglich; viele Formatierungen und Excel-spezifische Dokument-Eigenschaften gehen allerdings beim Speichern im ODS-Format verloren (Mic10c). Die Kompatibilität von mit Excel erstellten ODS-Dateien zum ODF-Standard stellt sich ähnlich dar wie bei Word – auch hier werden dieselben zwei Einträge in der Manifest-Datei vom ODF Validator als nicht Standard-konform kritisiert. Bei einer Testdatei mit mehreren Arbeitsblättern, Formeln, Grafiken und Diagrammen wurde für ODF v1.0 außerdem 9 x der unerlaubte Tag-Name „svg:title“ bemängelt. Vor einem breiten Einsatz von Excel mit dem Standard-Dateiformat ODS sollten möglichst viele typische Tabellenkalkulationen der jeweiligen Behörde auf den Erhalt der wesentlichen Eigenschaften hin, insbesondere der Formeln geprüft werden.

Abwärtskompatibel ist Excel 2010 nur teilweise, denn es lassen sich zwar XLS-Dateien öffnen und bearbeiten, solche im OpenOffice 1.x Dateiformat SXC allerdings nicht. In dieses Format lässt sich eine Excel-Tabelle auch nicht exportieren, in ODS, PDF, CSV, HTML und XLS hingegen schon. Analog zu Word können neu in Excel 2010 hinzugekommene Funktionalitäten nur im XLSX-Format gespeichert werden, bei jedem anderen Format gehen sie verloren. Abgesehen davon ist sowohl mit LibreOffice als auch mit MS Office 2003 ein Anpassen der Standardinhalte von aus Excel 2010 in die Formate ODS bzw. XLS exportierten Dateien möglich. In PDF kann exportiert werden, allerdings ist es beispielsweise nicht möglich, das Ergebnis im Querformat zu speichern. Beim HTML-Export werden die Inhalte der Arbeitsblätter analog zur Excel-Darstellung auf einzelnen Seiten abgebildet und über Hyperlinks verknüpft. Diagramme und Bilder werden beim Export berücksichtigt, erstere geraten allerdings sehr groß.

**LibreOffice Calc** weist hinsichtlich der Medientypenunterstützung und des automatischen Fortführens von Zelleninhalten dieselben Eigenschaften auf wie Excel. Dasselbe gilt für das Suchen in Tabellen, die Sortierfunktionen und das Filtern von Daten. Bei der Formelerstellung bietet Calc ebenfalls sehr viele vorgefertigte Funktionen und einen Formel-Assistenten an. Lediglich mit einem Formel-Debugger wie bei Excel kann Calc nicht aufwarten.

Umfangreiche Dokumente können mit Calc ebenso problemlos gehandhabt werden wie mit Excel. Eine Tabelle mit 5000 Zeilen und 6 Spalten lässt sich öffnen, sortieren, filtern und speichern. Trotz der vorhandenen Möglichkeit sollte man bei solch umfangreichen Dokumenten die Ablage des Inhalts in einer Datenbank erwägen, auf die dann auch andere Benutzer parallel zugreifen und dieselben Daten performant und ohne zwischengeschalteten E-Mail-Versand nutzen können.

In Calc können Diagramme eingefügt und verwaltet werden. Dabei existieren viele Gestaltungs- und Formatierungsoptionen, die der Vielfalt von MS Excel allerdings nur nahekommen. Trotzdem erscheint der verfügbare Funktionsumfang für den alltäglichen Bedarf als ausreichend.

Calc speichert Tabellen im ODS-Format, je nach Einstellung im Format ODF v1.2 oder ODF 1.0 / 1.1. Hinsichtlich der Schema-Validierung treten bei der mit Calc erstellten Testdatei mit Formeln, Bildern und Diagrammen gemäß ODF Validator für alle ODF-Versionen Fehler auf. In der Einstellung ODF 1.0 / 1.1 werden für beide ODF-Versionen jeweils 4 x nicht erlaubte Werte für das Attribut „chart:label-cell-address“, bei der strikten Validierung zudem 2 x nicht erlaubte Werte für das Atrtibute „style:text-position“ bemängelt. Letztere beide werden auch in der Einstellung ODF v1.2 kritisiert; zusätzlich wird 4

x der nicht erlaubte Tag-Name „chartooo:coordinate-region“ als Fehler festgestellt. Office-o-tron hingegen meldet auch in diesem Fall keine Validitäts-Verletzungen[189].

Zudem unterstützt Calc das Office Open XML Spreadsheet (XLSX)-Format insoweit, als Daten und Diagramme sowie Standard-Formeln wie WURZEL oder SUMME vollständig und korrekt gelesen werden und Formeln als solche erhalten bleiben. Auch eine Änderung von Grafiken, Bildern und Diagrammen in XLSX-Dateien und das Speichern in diesem Format ist mit Calc möglich. Insgesamt fallen bei der Tabellenkalkulation weniger Schwierigkeiten beim Bearbeiten gemeinsamer Dokumente durch Excel und Calc auf als bei den Textverarbeitungs-Pendants.

Hinsichtlich der Abwärtskompatibilität ermöglicht die LibreOffice-Komponente das Öffnen und Bearbeiten von XLS-Dokumenten einschließlich der Formelerstellung und des Einfügens von Diagrammen. Auch Grafiken und Bilder können bearbeitet, zugeschnitten und verschoben werden. Ebenfalls keine Probleme gibt es beim Öffnen und Bearbeiten von SXC-Dateien. Hier können Diagramme, Bilder und Formeln angepasst und hinzugefügt werden.

Ein Export in HTML ist möglich, Inhalte einzelner Tabellenblätter werden durch Querstriche getrennt untereinander dargestellt. Diagramme und Bilder werden berücksichtigt, erscheinen allerdings teilweise vervielfacht. Beim Exportieren in PDF bietet Calc einige Einstellungsmöglichkeiten an, beispielsweise das PDF mit einem Passwort zu versehen oder die Qualität der integrierten JPEG-Grafiken zu regulieren. Der Export in XSL und SXC funktioniert einwandfrei.

Tabelle 4.13: Vergleich Tabellenkalkulation

| Office-Komponente | MS Excel 2010 | LO Calc 3.4 |
|---|---|---|
| **Basisfunktionalität** | | |
| Medienunterstützung | ✓ | ✓ |
| Formelerstellung | ✓ | ✓ |
| Formel-Debugger | ✓ | - |
| Automatisches Fortführen von Zelleninhalten | ✓ | ✓ |
| Datensätze sortieren/filtern/suchen | ✓ | ✓ |
| Support großer Dokumente | ✓ | ✓ |
| Einfügen/Verwalten von Diagrammen | ✓ | ✓ |
| **Formatunterstützung** | | |
| ODF v1.0 | - | - |
| ODF v1.1 | ✓[190] | ✓[191] |
| ODF v1.2 | - | ✓[192] |
| **Abwärtskompatibilität** | | |
| XLS | ✓ | ✓ |
| Excel 2007 XML (Quasi-XLSX) | ✓ | ✓[193] |
| SXW | - | ✓ |

[189] Die Prüfung einer in ODF v1.2 gespeicherten ODS-Datei ergibt bei nicht gesetzter Option „Force validation of ODF against ISO/IEC 26300“ statt eines Validierungs-Ergebnisses eine java.lang.NullPointerException.
[190] Konformitäts-Fehler, siehe Seite 141
[191] Konformitäts-Fehler, siehe Seite 141
[192] Dieselben Konformitäts-Fehler wie für ODF v1.1.
[193] Geringe Interoperabilität

| Office-Komponente | MS Excel 2010 | LO Calc 3.4 |
|---|---|---|
| **Exportfunktion** | | |
| PDF / PDF/A | ✓/✓[194] | ✓/✓ |
| CSV | ✓ | ✓ |
| HTML 4.01 | ✓[195] | ✓[196] |

#### 4.3.4.5.6 Präsentation

Präsentationen werden häufig mit multimedialen Inhalten erstellt. Die entsprechende Komponente der Office-Suiten sollte dies daher ebenso beherrschen wie die anhand von Quervergleichen gängiger Office-Software ermittelte Basisfunktionalität. Zusätzlich dazu wurden aus einem Standard zur Erstellung von Multimedia-Präsentationen elementare Anforderungen abgeleitet (B+08).

**PowerPoint 2010** erlaubt das Einfügen und umfangreiche Bearbeiten vieler für Präsentationen wichtiger Medienformate (Mur04), darunter JPEG, GIF, PNG, SVG, Audio Video Interleave (AVI), MPEG-4 Part 14 (MP4) und Quicktime Movie (MOV). Objekte können per Drag & Drop oder per Koordinateneingabe positioniert und an einem Gitternetz oder an anderen Objekten ausgerichtet werden. Motion Picture Experts Group Standard 2 (MPEG-2)-Videos stellt PowerPoint nicht dar, Abspielbare Adobe-Flash-Animationen (SWF)-Dateien lassen sich zwar einfügen, aber nicht ohne Weiteres in die Datei einbetten (B+10). Es können mehrere kontinuierliche Medien (Audio, Video) in eine „Folie“ eingefügt werden. Deren bedingtes Abspielen (z.B. Start der Audio-Datei nach Ende des Videos) ist allerdings nicht möglich. Hyperlinks können für Formen und Grafiken, aber nicht für Videos definiert werden. PowerPoint unterstützt große Dokumente mit vielen eingebetteten Objekten und bietet beim Einfügen von Tabellen und Diagrammen viele Gestaltungs- und Formatierungsmöglichkeiten.

Bei der Formatunterstützung zeigt sich dasselbe Bild wie bei den bisher beleuchteten Komponenten – sobald ein anderes Format als Office Open XML Presentation (PPTX) zum Speichern verwendet wird, gehen die jüngsten Powerpoint-Spezifika ebenso verloren wie diverse Formatierungen und Positionierungen. In Folien enthaltene Tabellen werden beim Speichern als OpenDocument Presentation (ODP) in Bilder gewandelt und sind folglich nicht mehr änderbar. Kopf- und Fußzeilen werden zu reinen Textfeldern gewandelt, Kommentare nicht unterstützt. Mit Letzterem fehlt eine wesentliche Funktion für das gemeinsame Bearbeiten.

Die Prüfung der Standardkonformität von mit Powerpoint erstellten ODP-Dateien mit dem ODF Validator ergibt neben den beiden stets kritisierten Manifest-Einträgen für ODF v1.1 ein Fehler[197], für ODF v1.0 weit über Tausend[198]. Die Konformität zu ODF v1.1 ist daher fraglich, zu ODF v1.0 nicht gegeben.

Auch das Einlesen von ODP-Dateien führt teilweise zu Verlusten gegenüber dem Original. Beispielsweise ist das Bearbeiten von Datenquellen für Diagramme in ODP-Dateien nicht möglich, das von Bildern, Texten oder Überschriften hingegen schon. Microsoft bietet eine Übersicht über die nicht, teilweise oder vollständig unterstützten Eigenschaften von OOXML und ODF (Mic10d).

Ansonsten kann Powerpoint Dateien im früheren Microsoft Office Powerpoint Binärformat (PPT)-Format lesen und schreiben, SUN XML Impress (SXI)-Dateien hingegen nicht. Der PDF-Export funktioniert einwandfrei, ein Export in HTML wird nicht angeboten. Wie bei den anderen Microsoft Office Komponenten gilt auch für Powerpoint eine auf die eigene Produktreihe eingeschränkte Abwärtskompatibilität.

[194] Eingeschränkte Steuerungsmöglichkeiten beim PDF-Export.
[195] Diagramme erscheinen unverhältnismäßig groß.
[196] Teilweise mehrfacher Export derselben Diagramme und Bilder.
[197] „Error: id18 is used as an ID value more than once.“
[198] Hauptsächlicher Fehler ist der unerlaubte Tag-Name „svg:title“.

**LibreOffice Impress** erlaubt das Einfügen zahlreicher Medientypen, darunter Bildformate wie JPEG, GIF und PNG, Grafikformate wie SVG und Videoformate wie MP4, MOV und AVI; Windows Media Video (WMV)- und SWF-Dateien können nicht eingefügt werden. Objekte können wie bei Powerpoint positioniert und ausgerichtet werden. Das bedingte Abspielen kontinuierlicher Medien ist auch mit Impress nicht möglich, entsprechende Objekte werden mit dem Anzeigen der Folie gestartet. Mit Impress können Hyperlinks für Formen, Grafiken und Videos definiert werden, umfangreiche Dokumente werden problemlos unterstützt. Gleiches gilt für das Einfügen von Tabellen und Diagrammen, bei denen die üblichen Gestaltungs- und Formatierungsmöglichkeiten existieren.

Impress kann neben dem ODP-Format auch PPTX-Dateien lesen und schreiben, wenn auch mit den bereits oben genannten Unzulänglichkeiten wie abweichender Positionierung von Grafiken oder Schriftgrößen. Bei komplexeren Präsentationen kommt es allerdings häufig vor, dass Powerpoint mit Impress erstellte PPTX-Dateien nicht (mehr) lesen kann.

Die Prüfung der Standardkonformität von mit Impress erstellten ODP-Dateien mit dem ODF Validator ergibt für ODF v1.2 diverse Fehler[199], für ODF v1.1[200] und ODF v1.0[201] gilt dasselbe. Eine Konformität von Impress zum ODF-Standard ist damit zweifelhaft.

SXI-Dateien können mit Impress vollständig gelesen und geschrieben werden. Dasselbe gilt weitgehend für Präsentationen im PPT-Format; Datenquellen von in PPT eingebetteten Diagrammen können allerdings nicht bearbeitet werden, und auch hier treten kleinere Formatierungsunterschiede gegenüber Powerpoint auf. Der HTML-Export bietet hervorragende Einstellungsmöglichkeiten zur Gestaltung der generierten Webseiten, auch beim PDF-Export können viele Eigenschaften justiert werden. Beide Export-Varianten liefern überzeugende Ergebnisse.

Tabelle 4.14: Vergleich Präsentation

| Office-Komponente | MS Powerpoint 2010 | LO Impress 3.4 |
|---|---|---|
| **Basisfunktionalität** | | |
| Medienunterstützung | ✓ | ✓ |
| Layout-Gestaltung | ✓ | ✓ |
| Zeitliche Synchronisation kontinuierlicher Medien | - | - |
| Interaktivität (Hyperlinks) | ✓ | ✓ |
| Support großer Dokumente | ✓ | ✓ |
| Einfügen/Verwalten von Diagrammen | ✓ | ✓ |
| Einfügen/Verwalten von Tabellen | ✓ | ✓ |
| **Formatunterstützung** | | |
| ODF v1.0 | - | - |
| ODF v1.1 | ✓[202] | ✓[203] |
| ODF v1.2 | - | ✓[204] |
| **Abwärtskompatibilität** | | |

[199] Unzulässige Tag-Namen „style:graphic-properties“ und „chartooo:coordinate-region“, zudem „element draw:connector is missing viewBox attribute“
[200] Unzulässige Tag-Namen „style:graphic-properties“ und „chartooo:coordinate-region“, unerwartetes Attribut „svg:d“
[201] Unzulässiger Tag-Name „style:graphic-properties“, unerwartete Attribute „svg:d“ und „xlink:hre“
[202] Konformitäts-Fehler, siehe Seite 143
[203] Konformitäts-Fehler, siehe Seite 144
[204] Konformitäts-Fehler, siehe Seite 144

| Office-Komponente | MS Powerpoint 2010 | LO Impress 3.4 |
|---|---|---|
| PPT | ✓ | ✓ |
| Powerpoint 2007 XML (Quasi-PPTX) | ✓ | ✓[205] |
| SXI | - | ✓ |
| **Exportfunktion** | | |
| PDF / PDF/A | ✓/✓[206] | ✓/✓ |
| HTML 4.01 | - | ✓[207] |

#### 4.3.4.6 Empfehlungen

Beide betrachteten Office-Suiten bieten vergleichbare Ansätze und ausgereifte Funktionalitäten zur Bewältigung üblicher Anforderungen einer Behörde sowie zur zentral gesteuerten Installation und zur Administration von Einstellungen. Auch unterstützen beide formal das vom IT-Rats-Beschluss geforderte OASIS Open Document Format for Office Applications (ODF). Sie unterscheiden sich allerdings stark im äußeren Erscheinungsbild, der Bedienung und vor allem in der konkreten Umsetzung des Lesens und Schreibens der relevanten Dokumentenformate. Es zeigt sich selbst bei einfachen Testfällen, dass die Interoperabilität zwischen verschiedenen Office-Suiten auf der Basis bearbeitbarer Dokumente nur rudimentär gegeben und selbst beim Einsatz verschiedener Versionen derselben Produktfamilie nicht garantiert ist.

Daher sollte auf den Versand von Office-Dokumenten zugunsten von PDF möglichst verzichtet werden. Bei der Interaktion mit anderen Behörden oder Privaten sollte geprüft werden, inwieweit auch künftig *änderbare Dokumentenformate* (Die11b) versandt und empfangen werden *müssen*. Sinnvoll ist dies lediglich beim gemeinsamen Verfassen von Dokumenten; das verteilte strukturierte Erfassen von Daten hingegen sollte über dafür vorgesehene (Fach-)Anwendungen und Web-basierte Schnittstellen umgesetzt werden. Vermieden werden sollte das (übergangsweise) Versenden von Dokumenten in mehreren änderbaren Dokumentenformaten, da einerseits derzeit keine vollständige Konversionsmöglichkeit insbesondere zwischen ODF und OOXML besteht (EZI09) und andererseits besondere Sorgfalt für die Gewährleistung derselben Inhalte und derselben Darstellung notwendig ist. Für den reinen Informationsaustausch ist das Portable Document Format (PDF) derzeit das sinnvollste Dokumentenformat.

Das gemeinsame Bearbeiten von Textdokumenten sollte beim Einsatz verschiedener Office-Suiten oder unterschiedlicher Versionen so gestaltet werden, dass während der Erarbeitung der Inhalte auf Formatierungen und aktive Inhalte zugunsten der Interoperabilität verzichtet wird und möglichst nur strukturierende Elemente wie Überschriften, Tabellen und Listen verwendet werden. Die Änderungsverfolgung ist beim Einsatz von Microsoft Office nur im eigenen OOXML-Format möglich und wird für ODF ausgeschlossen. Daher sollte vorab zudem festgelegt werden, in welchem Format die gemeinsam bearbeiteten Dokumente von allen Beteiligten zu speichern sind. Hilfsmittel wie Kommentare oder eine Änderungsverfolgung können nur dann verlässlich eingesetzt werden, wenn alle Beteiligten mit derselben Version derselben Office-Suite arbeiten. Beim gemischten Einsatz von Libre- und Microsoft Office sollte ein Rückgriff auf frühere Formate wie DOC oder RTF geprüft werden, da hier derzeit eine bessere Interoperabilität gegeben ist als bei der Verwendung von ODF oder OOXML.

Eine gleichzeitige ablösende Migration aller Arbeitsplätze einer Behörde zur künftigen Office-Suite ist angesichts des erforderlichen Schulungs-, Administrations- und Betreuungsaufwands nicht sinnvoll zu bewältigen. Vielmehr sollten die Arbeitsplätze in fachlich eng zusammenarbeitende Gruppen geschnitten und gruppenweise migriert werden. Die dabei anfangs gewonnenen Erkenntnisse und Erfahrungen

[205] Geringe Interoperabilität
[206] Eingeschränkte Steuerungsmöglichkeiten beim PDF-Export.
[207] Sehr gute Steuerungsmöglichkeiten beim HTML-Export.

sollten von einem Projektbüro gesammelt, konsolidiert und in ein Vorgehensmodell überführt werden, welches an Multiplikatoren weitergegeben werden kann. Zur Gewährleistung der Zusammenarbeit mit noch nicht migrierten Gruppen oder Externen sollten obige Empfehlungen zur Interoperabilität berücksichtigt werden.

Dokumente in aus Sicht der derzeitigen Office-Suite bereits veralteten Formaten gilt es dahingehend zu überprüfen, ob sie weiterhin empfangen und/oder bearbeitet werden müssen. Ist dies der Fall, müssen auch diese Formate unterstützt werden. Allerdings sollten die Dokumente mittelfristig entweder automatisiert oder manuell mit der nächsten Bearbeitung in das ODF überführt werden. Die ggf. am Datenaustausch beteiligten Externen sollten darüber informiert werden, in welchem Zeitrahmen das bisherige veraltete Dokumentenformat durch ODF abgelöst werden soll. Ist keine Bearbeitung mehr zu erwarten, aber eine inhaltliche Archivierung vonnöten, sollten diese Dokumente in das Portable Document Format zur Langzeitarchivierung (PDF/A) überführt und in dieser Form archiviert werden; die bearbeitbare Form sollte anschließend zur Vermeidung von Inkonsistenzen gelöscht werden.

Vor einer Migration sollte die Handhabbarkeit der in einer Behörde am häufigsten benötigten Funktionen eines Office-Pakets ermittelt werden. Als Tester sollten Personen aus verschiedenen Abteilungen mit unterschiedlichen Office- und PC-Kenntnissen eingesetzt werden, um eine möglichst breite Akzeptanz sowohl bei den *Early Adopters* (frühen Anwendern) als auch der *Late Majority* (späten Mehrheit) zu erreichen (Rog62). Es sollte geprüft werden, ob die Testpersonen Dokumente mit für die jeweilige Behörde typischen Inhalten in den relevanten Formaten öffnen, bearbeiten und speichern können, und ob der Umgang mit verschiedenen Formaten ohne große Schwierigkeiten möglich ist.

Ebenfalls vor einer Migration sollte die Konvertierung von Dokumenten geklärt und insbesondere die Konformität zum künftigen Standard sowie eine möglichst hohe Layouttreue zum bisherigen Stand verifiziert werden. Da offizielle Prüfergebnisse zur Standardkonformität oder zur Layouttreue einzelner Produkte derzeit nicht verfügbar sind, sollten möglichst viele musterhafte Dokumente der Behörde mit geeigneten Werkzeugen wie dem ODF Validator oder OfficeShots entsprechend geprüft werden.

Die Gefahr von Angriffen anhand präparierter Office-Dateien ist bei beiden Office-Suiten gegeben. Auch wenn die Zahl bekannter Schwachstellen seit Jahren rückläufig ist[208], existieren weiterhin Sicherheitslücken, durch die Angreifer Zugriff auf den Arbeitsplatzrechner oder das interne Netzwerk erlangen können. Die Gefahr kann zwar durch technische Maßnahmen wie Virenscanner, Firewalls mit Content Filter oder deaktivierte aktive Inhalte reduziert, aber nicht ausgeschlossen werden. Vor dem Öffnen empfangener Dokumente sollte daher stets geprüft werden, ob der Versender bekannt ist und der Eingang des Dokuments zu erwarten war. Zudem sollten zum Versand anstehende bearbeitbare Dokumente stets zuvor von aktiven Inhalten befreit werden. Eine weitere potentielle Gefahr stellen die Metadaten von Dokumenten (z.B. Bearbeitername, verwendete Software) dar, da aus ihnen sowohl auf organisatorische als auch auf technische Gegebenheiten samt bekannter Sicherheitslücken geschlossen werden kann[209]. Bei der Bereitstellung von Dokumenten sollten daher die Metadaten auf das notwendige Minimum reduziert und möglichst entsprechende Werkzeuge zentral bereitgestellt werden, die diese Filterung automatisieren.

#### 4.3.4.7 Migrations-Checkliste

Das sequenzielle Durchlaufen der nachfolgenden Checkliste stellt sicher, dass alle relevanten Aspekte bei der Migration einer Office-Suite berücksichtigt werden. Die unter den Arbeitsschritten stehenden Informationen zeigen, wie die Bewertungskriterien konkretisiert werden können. Die Checkliste geht beispielhaft von einer vierstelligen Zahl umzustellender Arbeitsplätze aus und ist an die konkrete Projektsituation anzupassen.

[208] Siehe beispielsweise http://heise.de/-1230655
[209] Siehe http://heise.de/-1229482

#### 4.3.4.7.1 Projektbüro einrichten

1. Planung der Migration
2. Einteilung der Behörde in Migrations-Gruppen
3. Erstellung von Prüflisten für die Ist-Analyse

#### 4.3.4.7.2 Ist-Analyse gruppenweise durchführen

1. Eingesetzte Office-Suiten samt Version und genutzten Komponenten
2. Genutzte Funktionalität, festgestellte Probleme und Funktionslücken
3. Standard-Dokumentenformate, zusätzlich benötigte Formatunterstützung für Abwärtskompatibilität oder Export
4. Erfassen von Eigenentwicklungen, Erweiterungen und betroffenen Fachverfahren
5. Domänenspezifische Bewertungskriterien

#### 4.3.4.7.3 Ist-Analyse auswerten

1. Liste mit Mindest-Anforderungen an die Basisfunktionalität
2. Liste mit spezifischen Zusatz-Anforderungen
3. Priorisierung der Anforderungen
4. Konsolidierung und Optimierung der gruppenweise gewonnenen Erkenntnisse, z.B. Zusammenführen ähnlicher Dokumentvorlagen u.ä.

#### 4.3.4.7.4 Soll-Konzeption durchführen

1. Zuordnung der einzelnen Anforderungen zum umsetzenden Teilsystem
2. Festlegen des Standard-Dokumentenformats
3. Frühzeitige Information Externer über künftiges Standard-Dokumentenformat
4. Ggf. Produktsichtung Metadaten-Filter
5. Übergabe von Desktop-Datenbanken an IT-Betrieb planen
6. Zentrale Bereitstellung von Dokumentvorlagen, Skripten u.ä. mit IT-Betrieb abstimmen
7. Domänenspezifika festlegen (z.B. benötigte Integrationsfähigkeiten der Textverarbeitung, Erweiterungen zur Unterstützung von XÖV-Formaten)

#### 4.3.4.7.5 Bewertung und Entscheidung

1. Vorauswahl der Prüfkandidaten
   Anhand der oben vorgestellten Office-Alternativen unter Berücksichtigung der jeweils aktuellen Version
2. Abgleich der Mindest-Anforderungen an die Basisfunktionalität mit Funktionalitäten der Produkte
3. Abgleich der spezifischen Zusatz-Anforderungen mit Funktionalitäten der Produkte

4. Test der Dokumentkonvertierung anhand von Musterdokumenten hinsichtlich Standardkonformität und Layouttreue
5. Gewichtung der Bereiche Basisfunktionalität, Formatunterstützung, Abwärtskompatibilität, Exportfunktion und domänenspezifischer Bewertungskriterien (Summe der Gewichtungen = 100%)
6. Eintragen der Bewertungsergebnisse der Bereiche
7. Ermitteln des Gesamtergebnisses durch Multiplikation der Gewichtung und des Bewertungsergebnisses je Bereich für alle betrachteten Alternativen

## 4.3.5 Dokumenten Management Systeme

### 4.3.5.1 Einleitung

Nahezu jeder Arbeitsplatz einer Behörde ist heutzutage mit einem Computer ausgestattet. Dementsprechend hoch ist die Anzahl an Dokumenten mit codierten Informationen (Codierte Informationen (CI)). Dazu kommen Dokumente mit nicht-codierten Informationen (Nicht-codierte Informationen (NCI)) wie Akten, Briefe, Memos oder Aktenscans. Insgesamt besteht eine enorme Menge an Dokumenten, die es zu verwalten gilt, denn ansonsten würden viele Informationen mehrfach erarbeitet und abgelegt.

Digitale Unterstützung für diese Aufgaben bieten Dokumenten-Management-Systemes (DMSs), deren Funktionsumfang kontinuierlich zunimmt und optimiert wird. Folglich ist das Potential vorhanden, Prozessoptimierungen und somit Kosteneinsparungen bei der Migration auf neue DMS zu realisieren. Dabei sind diverse Aspekte zu beachten, die in den folgenden Abschnitten behandelt werden.

### 4.3.5.2 Kriterienkatalog

Dokumente durchlaufen einen Lebenszyklus mit mehreren Phasen. Zum Management dieser Phasen fallen verschiedenen Aufgaben an, bei denen der Anwender vom DMS unterstützt werden muss. Die folgenden, am Software- und Kriterienkatalog zu RAfEG – Referenzarchitektur für E-Government angelehnten Ausführungen zeigen, welche Bewertungskriterien pro Phase relevant sind. Die enthaltenen Zitate sind, soweit nicht anders gekennzeichnet, (B$^+$05) entnommen.

#### 4.3.5.2.1 Erfassen

„CI–Dokumente [...] und NCI-Dokumente [...] müssen von einem DMS [...] erfasst werden können. Neben dem eigentlichen Dokument müssen zusätzliche Informationen erfassbar sein.“ Das Ziel hierbei ist, dass in externen Anwendungen erstellte bzw. erfasste Dokumente (z.B. per Dokumentenscanner) über das DMS verwaltet werden.

#### 4.3.5.2.2 Speichern

Erfasste Dokumente müssen in einem **Datenspeicher abgelegt** werden, damit sie auch weiterhin zur Verfügung stehen. Dies gilt allerdings nur, bis sie nicht mehr aktiv genutzt werden. Danach werden sie je nach Rechtslage gelöscht oder langzeitarchiviert.

#### 4.3.5.2.3 Kontrolle und Freigabe

Nach der Dokumentenerfassung und -speicherung sind die Dokumente auf Inhalt und Struktur zu überprüfen. Dadurch wird die Einhaltung eines behördenspezifischen Qualitätsstandards sichergestellt. Anschließend können die Dokumente freigegeben werden, d.h. sie sind für andere Anwender auffindbar.

#### 4.3.5.2.4 Langzeitarchivierung

„Verfallende Dokumentenversionen werden vom DMS archiviert. Zu einem späteren Zeitpunkt können die Dokumente dann wiederhergestellt werden, um bspw. für eine Revisionsprüfung bereitzustehen oder eine fälschlicherweise neuere Version des Dokumentes zu ersetzen.“

#### 4.3.5.2.5 Suche und Änderung

„Zur [...] [Änderung] eines Dokumentes muss dieses mit Hilfe einer Suchfunktion und anhand diverser Merkmale vom Benutzer auffindbar sein.“ Die tatsächliche Änderung der Inhalte geschieht in externen Fachverfahren (Office-Anwendungen, E-Mail-Programmen etc.). Allerdings muss das DMS die Möglichkeit bieten, Metadaten (z.B. Querverweise auf anderer Dokumente) der Dokumente zu verändern. Nach der Änderung werden die Dokumente wieder gespeichert, kontrolliert und freigegeben.

#### 4.3.5.2.6 Sicheres Löschen

Überschreiten Dokumente ihre gesetzlich geregelte Aufbewahrungsfrist oder existiert keine Regelung und wird das jeweilige Dokument nicht mehr benötigt, kann es endgültig und sicher gelöscht werden.

Neben den Bewertungskriterien, die sich aus den Aufgaben eines DMS ergeben, existieren weitere Anforderungen die zu beachten sind.

#### 4.3.5.2.7 Dateiformate

In Behörden verwendete Dokumente liegen in vielen verschiedenen Formaten vor, die vom DMS zu unterstützen sind. Eine Umstellung auf andere Formate allein des DMS und seiner Fähigkeiten wegen ist nicht zu empfehlen, weil damit zu viel Aufwand verbunden wäre.

#### 4.3.5.2.8 Versionsverwaltung

Eine der wichtigsten Komponenten eines DMS ist die Versionsverwaltung. Durch sie wird es möglich, unterschiedliche Versionen von Dokumenten anzulegen, Änderungen an Dokumenten nachzuverfolgen, parallele und im Konflikt miteinander stehende Dokumentänderungen mit früheren Versionen zu vergleichen und Dokumente zu sperren. Dieses Modul ermöglicht also das kollaborative Arbeiten und verwalten von Dokumenten.

#### 4.3.5.2.9 Rollen- und Rechteverwaltung

Greifen mehrere Personen mit unterschiedlichen Zielen auf Dokumente zu, ist es sinnvoll, eine Rollen- und Rechteverwaltung zu realisieren. Dadurch verringert sich das Risiko inkonsistenter oder zerstörter Dokumente.

#### 4.3.5.2.10 Sicherheitsaspekte

In der Regel werden Dokumente auf einer zentralen Datenbasis über Netzwerk-Protokolle abgelegt. Teilweise werden aber auch Datenspeicher außerhalb der Behördengrenzen genutzt. Folglich existieren viele potentielle Schwachstellen, die es zu adressieren gilt.

#### 4.3.5.2.11 Workflow-Komponente

Das primäre Ziel des Dokumentenmanagements ist es, die Verwaltung unzähliger Dokumente zu vereinfachen. Bei dieser Verwaltung fallen viele Aufgaben an, welche sich kontinuierlich wiederholen, beispielsweise das Archivieren von Dokumenten, die eine bestimmte Lebensdauer überschritten haben. Gleicht sich dieser Prozess vom einen zum anderen Mal, ist eine Automatisierung vorteilhaft. Diese Automatisierung ist eine Aufgabe der Workflow-Komponente.

#### 4.3.5.2.12 Standards und De-facto Standards

„Die am Markt angebotenen Dokumentenmanagement- und Archivsysteme sind nicht alle miteinander kompatibel. Dies ist sowohl durch die verwendete Technologie als auch durch die verwendeten Medien- und Speicherformate verursacht. Um diese Probleme zu beheben, arbeiten die am Markt operierenden DMS-Hersteller in verschiedenen Gremien an der Vereinheitlichung der dem Dokumentenmanagement zugrundeliegenden Technologien zum Speichern und Wiedergewinnen von Dokumenten. Bei der Auswahl des DMS sollten die betreffenden Standards berücksichtigt werden, damit DMS- und Archivkomponenten langfristig verträglich sind.[210]“

[210] https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02259.html, abgerufen: 12.08.2011

#### 4.3.5.2.13 Administrationsoberfläche

Die bisher beschriebenen Aufgaben und Anforderungen lassen erkennen, dass mit einem DMS regelmäßig sehr viele Dokumente, Repositories und Nutzer zu verwalten sind. Diese Aspekte müssen über eine Administrationsoberfläche zentral zugänglich sein.

### 4.3.5.3 Methodik

#### 4.3.5.3.1 Ist-Analyse

Zunächst müssen die vom aktuellen DMS verwalteten **Dokumentenformate** bestimmt werden. Darüber weiß i.d.R. der für das DMS zuständige Administrator Bescheid. Kann diesbezüglich keine Auskunft gegeben werden, ist der nächste Anhaltspunkt das momentan eingesetzt DMS. Dort wird häufig eine Statistik über die verwalteten Dokumentenformate geführt. Steht auch diese Option nicht zur Verfügung, ist eine Dateiformaterkennung basierend auf der Dateiendung sinnvoll. Dieser Arbeitsschritt kann normalerweise leicht von einer Fachkraft automatisiert werden.

Neben der Formatanalyse ist auch eine Metadatenanalyse der Dokumente durchzuführen, d.h. es ist festzustellen, welche zusätzlichen Informationen (Autor, Erstellungsdatum etc.) momentan gespeichert werden. Besonders interessant ist hier die Geheimhaltungsstufe. Von ihr ist die jeweilige Ausprägung (geheim, streng geheim etc.) festzuhalten, denn davon hängen einige weitere Bewertungskriterien ab. Informationsquellen zur Durchführung dieses Schrittes sind die Statistiken im aktuellen DMS. Existieren diese nicht, können offene Dateiformate durch Algorithmen automatisch analysiert werden. Dazu ist i.d.R. eine individuelle Implementierung durch einen IT-Spezialisten nötig. Sind beide Arbeitsschritte nicht möglich, müssen die Dateien manuell geprüft werden. Bei der Auswahl der zu prüfenden Dateien bietet es sich an, unterschiedliche Dokumententypen zu selektieren. Beispielsweise ist es wahrscheinlich, dass Bilddateien andere Metadaten zugewiesen sind als Textdateien.

Stehen Art, Metadaten und Häufigkeiten der Dateiformate fest, sind die vom aktuellen DMS verwendeten **Datenspeicher** zu analysieren. Dabei spielen folgende Aspekte eine Rolle:

1. Version, Hersteller und vorhandene Schnittstellen des Datenspeichers, auch in Bezug auf die **Suche** nach Dokumenten. Durch diese Informationen ist ein Abgleich möglich, ob vorhandene Datenspeicher weiter verwendet werden können.
2. Anhand der Datenspeichervolumina kann abgeschätzt werden, ob generell ein Weiterverwenden möglich ist oder, falls nicht, wie groß das neue DMS zu dimensionieren ist.
3. Hard- und Software, die zum Betrieb des Datenspeichers zur Verfügung stehen. Handelt es sich beispielsweise um eine relationale Datenbank, ist zu prüfen, ob sie auf den zur Verfügung stehenden Applikationsservern respektive deren Betriebssystemen ausführbar ist.

Informationen über Art und Umfang des Datenspeichers sowie die existierenden Applikationsserver hat i.d.R. der zuständige Administrator. Die verfügbaren Schnittstellen der Datenspeicher gehen aus der jeweiligen Herstellerspezifikation hervor.

Gleiches gilt für die **Archivierung**. Auch hier sind die verwendeten Dateiformate, Umfang und Art des Datenspeichers sowie die Schnittstellen zum Ansprechen des Systems und zur Suche nach archivierten Dokumenten zu bestimmen. Informationen dazu finden sich in den Herstellerspezifikationen oder lassen sich vom Administrator beziehen.

Neben den Speichersystemen sind die Fachverfahren zur **Erfassung** und Bearbeitung von Dokumenten zu integrieren. Dies erleichtert das Arbeiten mit dem DMS, weil das Registrieren und Ablegen von Dokumenten im DMS direkt über das jeweilige Fachverfahren stattfindet. Folglich ist festzustellen, welche Anwendungen zur Erstellung von Dokumenten verwendet werden und ob diese einfach zu erweitern sind. Letzteres deswegen, weil eine native Anbindung an beliebige DMS i.d.R. nicht zum Funktionsumfang gängiger Dokumentenerstellungs-Werkzeuge gehört. Somit ist eine nachträgliche Erweiterung nötig.

Welche Erfassungs- oder Erstellungssoftware verwendet wird, geht einerseits aus der Ist-Analyse der Dokumentenformate (vgl. 4.3.5.3.1) und andererseits aus einer Befragung des Systembetriebs hervor. Alternativ ist auch eine Mitarbeiterbefragung möglich. Ob die Werkzeuge Erweiterungsmöglichkeiten bieten, ist über die jeweilige Herstellerspezifikation herauszufinden.

Ebenfalls zu analysieren sind die mit dem aktuellen DMS **automatisierten Workflows**. Dadurch wird ersichtlich, welche Abläufe das neue DMS mindestens automatisieren muss. Neben den Workflows ist auch deren Beschreibungssprache zu ermitteln. Wird sie vom Ziel-DMS unterstützt, können die Prozesse leichter wiederverwendet werden. Die momentan automatisierten Workflows sind über die Verwaltungskomponente des aktuellen DMS ersichtlich. Deren Beschreibungssprache ergibt sich aus den zu den Automatisierungen gehörenden Dateien im Datenspeicher oder aus der Herstellerspezifikation.

Im Rahmen der Ist-Analyse spielt im Kontext der **Administrationsoberfläche** das Monitoring eine zentrale Rolle. Über eine Befragung der Systemadministration ist festzustellen, welche Kennzahlen und Auswertungsmöglichkeiten das aktuelle DMS anbietet, welche davon genutzt werden und welche derzeit nicht verfügbar sind.

#### 4.3.5.3.2 Soll-Konzeption

Nachdem umfangreiche Informationen zum aktuellen DMS eingeholt wurden, sind die Anforderungen an das künftige Fachverfahren zu spezifizieren. Hier bietet sich wie bei jeder Soll-Konzeption ein enger Kontakt mit den derzeitigen Nutzern an, denn sie kennen die Schwächen des alten DMS und haben meist konkrete Vorstellungen, was ihre tägliche Arbeit erleichtern würde. Darüber hinaus sollten die folgenden Aspekte beachtet werden. Der übliche Mechanismus zur Kopplung von Erfassungs- oder Erstellungssystemen mit dem DMS (Office-Anwendungen, E-Mail-Clients oder Scanner-Software bzw. -Hardware) ist ein **Erfassen** von Dokumenten direkt über die externen Fachverfahren, z.B. in Form einer Schaltfläche „Im DMS ablegen“. Folglich ist zu prüfen, ob Erweiterungen für die Fachverfahren existieren, die es ermöglichen direkt mit dem Ziel-DMS zu interagieren. Informationen dazu bietet i.d.R. der Hersteller des DMS. Existieren keine Erweiterungen für die Erstellungs-Tools, sind sie zu implementieren. Das DMS muss folglich entsprechende Schnittstellen bieten und sollte sich dabei an allgemeine Schnittstellenstandards wie Web Services Description Language (WSDL) für eine Anbindung über Web Services oder an DMS-spezifische Standards wie Open Document Management API (ODMA) halten. Sind solche Schnittstellen nicht vorhanden, muss das DMS alternative Möglichkeiten zur Dokumentenerfassung bieten, beispielsweise über ein Web-Frontend mit integrierter Importfunktion.

Beim **Erfassen** von Dokumenten sind allerdings nicht nur das Dokument selbst, sondern insbesondere dessen Metadaten relevant. „In der Regel sind dies Dokumenttyp, -kategorie, -status, Zugriffs–/Bearbeitungsrechte, Querverweise auf andere Dokumente, Notizen und weitere Informationen. ((B$^+$05))“. Ob die genannten Metadaten für den geplanten DMS-Einsatz ausreichen, hängt von Freigabeprozessen, gesetzlichen Regelungen und sonstigen gewünschten Funktionen ab und muss individuell geprüft werden. Die Metadaten sind ggf. zu erweitern. DMS-spezifische Metadaten, die z.B. eine Versionierung erlauben, müssen den Dokumenten bei deren Erfassung automatisch vom DMS zugewiesen werden.

Nach oder parallel zur Erfassung werden Dokumente im Datenspeicher des DMS **gespeichert**. Die vom künftigen DMS zu erfüllenden Anforderungen ergeben sich zunächst aus der Ist-Analyse. Die dort identifizierten Speichersysteme sind auf Wiederverwendbarkeit, also Integrierbarkeit mit dem DMS zu überprüfen. Dazu ist festzustellen, ob die bisherigen Datenspeicher für eine fortführende Verwendung ausreichend dimensioniert und performant sind. Aus Statistiken des aktuellen DMS zu gelöschten und hinzugekommenen Dateien lassen sich Trends für den zu erwartenden Dokumentenzuwachs ableiten. Diese Trends sollten als untere Richtgröße für die zunehmende Digitalisierung und den entsprechenden Zuwachs angesehen und ggf. nach oben korrigiert werden, sofern Maßnahmen wie die Einführung einer elektronischen Akte oder großflächige Dokumentenscans anstehen. Bietet das aktuelle DMS keine solchen Statistiken, sollten Log-Files von Servern und Speichersystemen ausgewertet werden.

Ein elementares Ziel des Dokumentenmanagements ist es, einen zentralen Zugriffspunkt auf Dokumente zu bieten. Daher sind neben dem künftigen Speichervolumen auch die Zugriffsmöglichkeiten auf den Speicher durch die vom DMS verwalteten Nutzer zu prüfen. Dies ist primär eine Berechtigungsfrage, folglich ist der Verwalter der Datenspeicher zu kontaktieren. Darüber hinaus sind aber auch die von den Speichersystemen angebotenen Schnittstellen- und Zugriffsstandards relevant. Sie wurden bei der Ist-Analyse (vgl. Abschnitt 4.3.5.3.1) bestimmt und sind nun auf Kompatibilität mit dem Migrationsziel zu überprüfen. Zusätzlich zu den Schnittstellen der Altsysteme sollte das künftige DMS weitere verfügbare Speichersysteme ansprechen können. Relevante Standards hierfür sind LDAP, CIFS und Web-based Distributed Authoring (WebDAV). Darüber hinaus ist zu prüfen, ob die vorliegende Hard- und Softwarelandschaft einen Betrieb des vorgesehenen DMS-Speichers und des DMS selbst zulässt.

Im Rahmen der **Kontrolle und Freigabe** legt der in der Behörde übliche oder vorgeschriebene Freigabeprozess für Dokumente die Anforderungen fest. Dieser muss in der **Workflow-Komponente** des künftigen DMS umsetzbar sein.

Analog zu den Speichersystemen für aktive Dokumente ist bei vorhandenen **Archivsystemen** zu prüfen, ob das künftige DMS damit integriert werden und ob das Archivsystem die zu erwartenden Datenmengen des DMS bewältigen kann. Die Integration des DMS mit dem Archivsystem sollte über gängige Schnittstellenstandards wie Web-Technologien (WSDL, REST) oder RPC[211] möglich sein. Besteht keine solche Integrationsfähigkeit, muss das DMS eine eigene Möglichkeit zur Langzeitarchivierung aufweisen, entsprechende Datenvolumina verlässlich verwalten können und mindestens die zur Langzeitarchivierung laut SAGA 5 relevanten Standards PDF/A und Extensible Markup Language (XML) für Text, JPEG und Tagged Image File Format (TIFF) für Bilder(Die11b) unterstützen. Darüber hinaus muss das DMS einige vom BSI definierte Anforderungen erfüllen[212].

Für die **Suche** nach Dokumenten sollten die künftig relevanten **Dateiformate** vom DMS für eine Volltextrecherche ausgewertet und die Suchfunktionen vorhandener Speicher- und ggf. Archivsysteme eingebunden werden können. Derzeit relevante Dateiformate sind PDF, PDF/A-1, OOXML, ODF(Die11b), die veralteten Microsoft Binärformate sowie weitere in der Ist-Analyse ermittelte Formate. **Geändert** werden Dokumente i.d.R. in Anwendungen außerhalb des DMS. Die Aufgabe des DMS ist es hierbei, die zur Änderung nötige Anwendung zu öffnen oder zumindest darauf hinzuweisen, welche Anwendung verwendet werden muss. Einige DMS bieten in die Anwenderschnittstelle integrierte Editoren für verbreitete Dokumentenformate. Deren Möglichkeiten sollten mit den Anforderungen der entsprechenden Anwender abgeglichen und die resultierende Konsistenz der Dokumente und Weiterverwendbarkeit durch die Standard-Anwendung geprüft werden. Entsprechend leistungsfähige Editoren sind insbesondere bei kleineren Änderungen eine sinnvolle Alternative zur Verwendung der ansonsten notwendigen Anwendung.

Ist die Aufbewahrungsfrist verstrichen oder existiert keine und die Dokumente werden nicht mehr benötigt, können sie **sicher gelöscht** werden. Welche Maßnahmen dabei nötig sind, hängt von behördenspezifischen Regelungen und auch von der Geheimhaltungsstufe der Dokumente ab. Das BSI definiert hierzu konkrete Anforderungen an ein DMS[213].

Zur Ablage der Metadaten sind ebenfalls spezielle **Dateiformate** nötig, die entweder auf die assoziierten Dokumente verweisen oder sie beinhalten (Containerformat). Diese Formate sind i.d.R. von DMS zu DMS unterschiedlich. Daher sollte auf die Offenheit und den Aufbau des jeweiligen Formats geachtet werden. Basiert es auf XML und existiert dazu eine frei zugängliche Schemadefinition (gem. (Die11b) derzeit auf der Basis von XSD 1.0), ist dessen Weiterverwendung oder Transformation mit einfachen Mitteln möglich.

Metadaten werden u.a. von der **Versionsverwaltung** genutzt, beispielsweise hinsichtlich des Autors eines Dokuments. Sofern externe Werkzeuge zur Versionsverwaltung wie Subversion[214] genutzt wer-

[211] Remote Procedure Calls, beispielsweise Java Remote Method Invocation

[212] vgl. https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, abgerufen: 18.08.2011

[213] https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m02/m02167.html, abgerufen: 18.08.2011

[214] http://subversion.apache.org

den sollen, sind die entsprechenden Integrationsmöglichkeiten zu prüfen. Im Rahmen von Freigabeprozessen hinzugefügte Kommentare können von solchen Werkzeugen beispielsweise als „Commit“-Text hinterlegt werden und sollten vom DMS angezeigt werden können.

Das DMS muss eine **Rollen- und Rechteverwaltung** derart ermöglichen, dass die Aufbauorganisation einer Behörde oder Abteilung und die notwendigen Zuweisungen von Rollen und Rechten an die Mitarbeiter geeignet abgebildet werden kann. Insbesondere müssen Geheimhaltungsstufen und die daraus hervorgehenden Folgen (Bun80) hinterlegt werden können. Dies sollte prototypisch in einer Testinstallation geprüft werden.

Konkrete **Sicherheitsmaßnahmen** bei DMS hängen ebenfalls von dem in der Ist-Analyse bestimmten Geheimhaltungsgrad der Dokumente ab. Handelt es sich bei den Dokumenten um Verschlussachen gemäß §4 SÜG(Bun94), sind die in §36 und 37 der Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen-Verschlusssachenanweisung (VS-Anweisung- VSA) zu beachten(Bun06). Hierbei ist eine enge Zusammenarbeit mit dem BSI wichtig, da es Sicherheitsmaßnahmen zertifiziert und somit genau über aktuelle Schwachstellen und Gegenmaßnahmen Bescheid weiß. Zum Nachweis des entsprechenden Funktionsumfangs und einer sorgfältigen Implementierung ist ein direkter Kontakt zum Hersteller des DMS zu suchen.

Neben den oben angesprochenen Dokumentenstandards existiert mit dem DOMEA-Konzept(Bun05) und den damit assoziierten Anforderungskatalogen(Bun08) für Behörden eine Vorgabe für das Dokumentenmanagement mit entsprechenden Bewertungskriterien. Das DOMEA-Konzept wird allerdings derzeit überarbeitet und soll demnächst unter dem Namen „Konzept eVerwaltung“ veröffentlicht werden[215], weshalb weitere Ausführungen hierzu erst nach dessen Veröffentlichung sinnvoll sind.

Aufgrund der zentralen Stellung eines DMS und vielfältiger Anbindungen an weitere Teilsysteme ist das verlässliche Funktionieren der relevanten Integrationsaspekte für die Benutzerakzeptanz wesentlich und sollte daher ausführlich getestet werden. Bei diesen Tests sollten zudem die künftig benötigten Auswertungen und Darstellungsarten geprüft werden.

[215] http://www.verwaltung-innovativ.de/cln_047/nn_684678/DE/Organisation/domea__konzept/domea__konzept__node.html?__nnn=true, abgerufen: 11.08.2011

## 4.3.6 Web Content Management Systeme

### 4.3.6.1 Einleitung

Anwenderschnittstellen von Fachverfahren werden immer häufiger mit einem Web-Frontend sowohl für Endanwender als auch für Administratoren realisiert. Zudem wird das Internet immer mehr zum zentralen Distributionskanal für behördliche Informationen. Die Folgen sind ein zunehmender Umfang und eine steigende Komplexität der Web-Angebote von Behörden. Damit diese Komplexität handhabbar bleibt, sind Fachverfahren nötig, die das Verwalten der Internetauftritte und der Webinhalte vereinfachen.

Webinhalte bezeichnen alle Dokumente (HTML-Seiten, XML-Dokumente, etc.), Bilder (JPG, PNG, usw.), Videos sowie jeglichen Applikationscode (z.B. JavaScript oder PHP), der im Inter- oder Intranet publiziert und über den Browser angezeigt wird.

### 4.3.6.2 Kriterienkatalog

Gemäß der im Migrationsleitfaden verwendeten Definition eines Web-Content-Management-System (WCMS) ist der Administrator einer Webseite bei folgenden Aufgaben zu unterstützen:

- bei der **Erstellung** von Webinhalten und bei dessen Import aus Anwendungen (z.B. HTML-Editor),
- beim **Speichern** von Webinhalten,
- bei der **Kontrolle und Freigabe** von erstellten Webinhalten,
- beim **Publizieren** der erstellten und kontrollierten Inhalte,
- bei der **Archivierung** nicht mehr benötigter Webseiten und
- beim **Wiederfinden** und bei der **Änderung** aktiver oder archivierter Inhalte.

Zur Erfüllung dieser Aufgaben bieten moderne WCMS eine Fülle an Funktionen. Einige davon haben sich im Laufe der Jahre als De-facto-Standard etabliert und werden deshalb als Bewertungskriterien herangezogen.

#### 4.3.6.2.1 Erstellung

Die für Webseiten übliche Aufteilung in Inhalt/Struktur- und Layout-Dokumente führt dazu, dass ein WCMS zwei Editoren zur Erstellung von Webinhalten bieten muss: einen **Inhalts- und Strukturedi tor** sowie einen **Layout-Editor**. Damit müssen die von SAGA **erlaubten Dateiformate** für Inhalt/Struktur (insb. HTML 4.01, vgl. (Die11b)) und Layout-Dokumente (insb. CSS 2.1, vgl. (Die11b)) erstellt werden können. Bei der Erstellung ist eine **Unterstützung zur Erstellung BITV-konformer Webseiten** notwendig, denn die Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz ist seit dem 27.02.2002 für Webauftritte von Behörden verbindlich (Bun02).

Der Inhalts- und Strukturedi tor muss **Funktionen zur Suchmaschinenoptimierung** anbieten, um den Internetauftritt intern besser auffindbar zu machen oder ihn extern möglichst flächendeckend zu publizieren. Diese und viele weitere Funktionen werden häufig durch Skriptsprachen (derzeit v.a. JavaScript oder PHP) realisiert. Folglich muss der Inhalts- und Strukturedi tor einen **Skriptsprachen-Support** bieten. Weiterhin muss der Editor die Möglichkeit zum **Dateiimport** bieten, um Bilder in Webauftritte zu integrieren oder um Webinhalte aus anderen Anwendungen (z.B. externer HTML-Editor) einzubinden.

#### 4.3.6.2.2 Speichern

Sind die gewünschten Dokumente erstellt, müssen sie gespeichert werden. Dabei sind diverse Aspekte zu beachten, die als Bewertungskriterien für moderne WCMS gelten:

- Das WCMS muss eine **Speichermöglichkeit** oder eine Anbindung an eine vorhandenen Speichermöglichkeit zur Verfügung stellen.

- Mit dem WCMS erstellte Dateien müssen in **SAGA-konformen Dateiformaten** gespeichert werden.
- Das WCMS muss eine **Versionsverwaltung** so integrieren, dass alle Dokumente in ihren jeweiligen Versionen erhalten bleiben und wiederhergestellt werden können und zu jeder Speicherung festgehalten wird, wer wann was bei welchem Dokument verändert hat. Zudem muss ein inhaltlicher Vergleich mit älteren oder parallel weiterverarbeiteten Versionen des Dokuments darüber möglich sein. Aufgetretene Konflikte müssen geeignet dargestellt und über einen Editor behebbar sein. Können Konflikte oder Fehler nicht behoben werden, müssen ältere Versionen wiederhergestellt werden können.

#### 4.3.6.2.3 Kontrolle und Freigabe

Es muss ein Kontroll- und Freigabeprozess (z.B. das Vier-Augen-Prinzip) integrierbar sein, der vor dem endgültigen Publizieren zwingend durchlaufen werden muss, um ein ausreichendes Maß an inhaltlicher Qualität erreichen zu können. Folglich muss das WCMS eine **Workflow-Komponente mit Kontroll- und Freigabemechanismen** aufweisen oder integrieren können.

Eine weitere wichtige Funktion im Rahmen der Kontrolle und Freigabe ist eine **Vorschaufunktion**, mit der die Webseite so angezeigt werden kann, wie sie nach dem Kontroll- und Freigabeprozess aussehen würde. Diese Vorschau der Webseite darf der Allgemeinheit nicht zugänglich sein.

#### 4.3.6.2.4 Publizieren

Ist eine ausreichende Qualität des Webinhalts sichergestellt, muss er publiziert werden können. Das WCMS muss Möglichkeiten zum einfachen Anstoßen eines entsprechenden **Publikationsprozesses** bieten.

#### 4.3.6.2.5 Archivierung

Webinhalte, die länger nicht mehr aktualisiert wurden oder keine Zugriffe mehr aufweisen, sollten entweder mit neuen Inhalten gefüllt oder archiviert werden. Die Analyse der Aktualität und der Zugriffszahlen ist zumindest bei umfangreichen Webauftritten manuell nicht sinnvoll. Folglich müssen in der Workflow-Komponente (vgl. Abschnitt 4.3.6.2.3) Prozesse zum **automatischen Archivieren** und zur **automatischen Aktualisierungsaufforderung** definierbar sein. Da die Archivierung häufig von einem separaten Archivsystem übernommen wird, muss das WCMS mit solchen **Archivsystemen integrierbar** sein.

#### 4.3.6.2.6 Änderung

Im vorherigen Abschnitt wurde bereits aufgezeigt, dass Webinhalte häufig auf den neuesten Stand zu bringen sind. Dazu müssen als erstes die zu aktualisierenden Webinhalte gefunden werden. Folglich ist eine **Suchfunktion** vom WCMS anzubieten, die sowohl das Archivsystem als auch die aktuell publizierten Webinhalte durchsucht. Wird ein separates Produkt zur Archivierung genutzt, ist zu prüfen, ob die **Suchfunktion des WCMS mit der des Archivsystems kombinierbar** ist.

Sind die zu aktualisierenden Dokumente gefunden, müssen sie abhängig von ihrer Art (Struktur/Inhalt bzw. Layout) im entsprechenden Editor (vgl. Abschnitt 4.3.6.2.1) geöffnet werden. Dies schließt den Lebenszyklus eines Webinhalts, d.h. ab diesem Zeitpunkt sind die vorherigen Schritte wieder relevant.

Neben dem Ändern von Dokumenten kann auch ein Löschen oder Umbenennen der gefundenen Datei notwendig sein, beispielsweise zur Umsetzung von Namenskonventionen. Dafür muss das WCMS die **Versionsverwaltung** geeignet instruieren. Mit letzterer sollten zudem Kopien von Dateien derart erstellt werden können, um sie ab dem Zeitpunkt der Kopie unabhängig vom Original weiterzuführen (Abzweigung). Folglich ist auch eine enge Integration mit dem Speichersystem (vgl. Abschnitt 4.3.6.2.2) notwendig, denn alle genannten Operationen beziehen sich darauf.

Aus den soeben genannten Anforderungen an WCMS folgen weitere Bewertungskriterien, die im Folgenden erläutert werden.

#### 4.3.6.2.7 Rollen- und Rechteverwaltung

Die unterschiedlichen Aufgaben eines WCMS fordern eine detaillierte Zuweisung von Tätigkeiten zu Personen. Soll beispielsweise ein Freigabeprozess nach dem Vier-Augen-Prinzip realisiert werden, ist eine Aufteilung der Rechte in Redakteur und Kontrolleur sinnvoll. Hätte der Redakteur auch Freigaberechte, könnte der Freigabeprozess ignoriert werden. Folglich ist eine **Rollen- und Rechteverwaltung** notwendig, die die Aufbau- und Ablauforganisation der jeweiligen Behörde abbilden kann. Je komplexer das somit entstehende Rollenmodell wird, desto wichtiger ist eine einfache Verwaltung. Folglich ist auf **Übersichtlichkeit und einfache Bedienbarkeit** bei der Rollen- und Rechteadministration des WCMS zu achten. Dabei kann auch eine **Vererbungsfunktion** sinnvoll sein, z.B. wenn sich Nutzertyp A nur geringfügig von Nutzertyp B unterscheidet.

Sollte tatsächlich der Fall eintreten, dass die Rollen- und Rechteverwaltung nach der Migration nicht detailliert genug konfigurierbar ist, schaffen gängige WCMS Abhilfe durch das Anbieten von Erweiterungsmechanismen. Welche das sind und was dabei zu berücksichtigen ist, zeigt der folgende Abschnitt.

#### 4.3.6.2.8 Erweiterbarkeit

Zusätzlich zu einer ggf. fehlenden Detailtiefe der Rollen- und Rechteverwaltung fordert gerade die hohe Dynamik von Internettrends und -technologien eine hohe Flexibilität von modernen WCMS. Demzufolge ist dessen leichte **Erweiterbarkeit** notwendig, sei es durch das Vorsehen eines Erweiterungskonzepts bei der Implementierung (z.B. Modulkonzept von Drupal[216], abgerufen: 09.08.2011) oder durch einen offengelegten Quellcode. Unabhängig von der Realisierung ist zu beachten, dass das WCMS ohne viel Aufwand durch den Betreiber erweitert werden kann. Dadurch wird eine höhere Flexibilität und somit eine schnellere Reaktionsfähigkeit auf neu entstehende Distributionskanäle ermöglicht.

Die im WCMS-Bereich vorhandenen **Erweiterungsmechanismen** sind vielfältig und weisen jeweils spezifische Vor- und Nachteile auf. Bei deren Prüfung sollte aber auf eine detaillierte und zentral dokumentierte **programmierbare Anwendungsschnittstelle (API)** für den Zugriff auf die Basisfunktionalität geachtet werden.

Bei Erweiterungen des WCMS, aber auch bei der Erstellung von Webinhalten spielen Sicherheitsaspekte eine große Rolle. Genauer geht darauf der folgende Abschnitt ein.

#### 4.3.6.2.9 Sicherheitsmodul

Eine Analyse der zehn häufigsten Sicherheitsrisiken bei Webanwendungen zeigt, dass viele Probleme auf mangelhaftes Webseiten-Design zurückzuführen sind (vgl. (The10)). Folglich sollte das WCMS bei der Erstellung von Webinhalten den erstellten Quellcode auf **Sicherheitsrisiken prüfen** und **Verbesserungsvorschläge** unterbreiten. Ein weiterer zentraler Sicherheitsmechnismus, der zum Standard-Repertoire zählen muss, ist das **verschlüsselte Übertragen und Ablegen von Daten**. Dadurch wird der unbefugte Zugriff zusätzlich erschwert und somit das Vertrauen in den Webauftritt gestärkt.

#### 4.3.6.2.10 Administrationsoberfläche

Viele der soeben genannten Bewertungskriterien fordern eine umfangreiche Funktionalität des WCMS. Es ist beispielsweise notwendig, neue Anwender anzulegen, neue Funktionalität zu integrieren oder eine Anbindung an vorhandene Speicherstrukturen zu realisieren. Dafür ist eine umfangreiche **Administrationsoberfläche** notwendig, die komfortabel den Zugriff auf alle Einstellungsoptionen bietet.

[216] http://drupal.org/project/modules

#### 4.3.6.2.11 Migrationsunterstützung

Webauftritte von Behörden beinhalten schnell unzählige Folgeseiten (Subsites). Jede dieser Subsites kann Bilder, Skript-Code oder sonstige Webinhalte enthalten. Steht nun eine Migration an, müssen diese Daten vom neuen WCMS weiter verwaltet werden. Ein manuelles Importieren der Webinhalte bzw. ein Anpassen der Datenbasis ist nur bei Webauftritten mit wenigen Seiten möglich. Folglich ist vor der Migration zu prüfen, ob eine **Migrationsunterstützung** existiert, beispielsweise durch automatisierte Workflows (s. 4.3.6.2.3), durch beiliegende Skripte oder durch Anleitungen.

### 4.3.6.3 Methodik

#### 4.3.6.3.1 Ist-Analyse

Als erstes sind die aktuell vorhandenen Dateiformate der Webinhalte sowie deren Inhalt zu analysieren. Mit Hilfe von Server-Log-Files (vgl. Kapitel 4.3.2) oder in Absprache mit Redakteuren kann dadurch eine Liste von Formaten, Skript- und Programmiersprachen erstellt werden, die das neue WCMS unterstützten muss. Bei dieser Anforderungserhebung kann gleichzeitig ein Meinungsbild eingeholt werden, welche Funktionen bei den aktuell eingesetzten WCMS fehlen. Bei der Befragung können die oben beschriebenen Bewertungskriterien als Anhaltspunkt verwendet werden, z.B. indem gefragt wird, ob die Versionsverwaltung ein Vergleichen von konfliktären Dokumenten erlaubt (vgl. Abschnitt 4.3.6.2.2).

Neben den vorhandenen Dateiformaten ist auch der Datenspeicher für aktive sowie archivierte Inhalte zu analysieren. Dabei ist zu klären, in welchem Speichersystem Daten archiviert oder für den aktuellen Betrieb gespeichert werden (Produkt und exakte Versionsnummer, z.B. MySQL 5.5.15). Außerdem muss festgestellt werden, wie viele Daten der aktuell verwaltete Webauftritt beinhaltet und wie umfangreich der momentan benötigte Speicherplatz ist. Beide Informationen legen die minimalen Anforderungen für das neue WCMS fest. Danach ist festzustellen, wie die Daten untereinander und somit auch mit dem Webauftritt zusammenhängen. Alle Fragen sind in enger Zusammenarbeit mit den Administratoren des Rechenzentrums bzw. des Archiv- oder Web-Content-Management-Systems zu realisieren. Zur Dokumentation der Datenstruktur bieten sich Klassendiagramme der Unified Markup Language (UML) an.

#### 4.3.6.3.2 Soll-Konzeption

Im Rahmen der Ist-Analyse ist durch die Experteninterviews ein domänenspezifischer Soll-Zustand definiert worden. Dieser Soll-Zustand muss nun basierend auf den in Kapitel 4.3.6.2 genannten Bewertungskriterien erweitert werden.

Bezüglich des gewünschten Funktionsumfangs der beiden notwendigen **Editoren** (vgl. 4.3.6.2.1) ist eine enge Zusammenarbeit mit den Redakteuren unverzichtbar. Falls dies noch nicht im Zuge der Ist-Analyse realisiert wurde, sollte eine Anforderungserhebung diesbezüglich durchgeführt werden. Dabei können auch allgemein gewünschte Funktionen des WCMS abgefragt werden. Eine Übersicht über die Funktionalitäten einzelner WCMS bietet die Webseite http://www.cmsmatrix.org/ (abgerufen: 10.08.2011).

Bei der Erstellung von Webinhalten stehen die **Datenformate** im Fokus. Das neue WCMS muss auf alle Fälle die bisher verwendeten Formate für Struktur/Inhalt bzw. Layout-Dokumente unterstützen (siehe Ist-Analyse). Zusätzlich dazu können wie in Abschnitt 4.3.2.3 künftig relevante Formate bestimmt werden.

Anforderungen hinsichtlich der **Unterstützung zur Erstellung BITV-konformer Webseiten** ergeben sich aus der Anlage 1 (zu § 3 und § 4 Absatz 1) der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (vgl. (Bun02)).

Notwendige **Funktionen zur Suchmaschinenoptimierung** sind davon abhängig, wie die Ranking-Algorithmen gängiger Suchmaschinen realisiert sind. Diese Informationen stellen die Suchmaschinenanbieter i.d.R. nicht zur Verfügung. Sie bieten allerdings häufig Tipps und Tricks[217] [218] auf ihren Web-

[217] http://www.google.de/webmasters/docs/einfuehrung-in-suchmaschinenoptimierung.pdf oder
[218] http://www.bing.com/toolbox/webmaster, abgerufen: 09.08.2011

seiten, wie die Bewertung des Webauftritts verbessert werden kann. Aus diesen Informationen lassen sich die zentralen Funktionen zur Suchmaschinenoptimierung ableiten und sollten über das WCMS umgesetzt werden können.

Welche **Skriptsprachen zu unterstützen sind**, geht aus der oben beschriebenen Analyse der relevanten Datenformate hervor. Ob die Editoren des neuen WCMS die relevanten Dateien **importieren** können, sollte über einen entsprechenden Funktionstest geprüft werden. Gleiches gilt für den Funktionsumfang der integrierten **Versionsverwaltung**.

Soll-Anforderungen bzgl. der **Speichermöglichkeit und der Anbindung an eine vorhandenen Speichermöglichkeit** können nur definiert werden, wenn eine Datenmigration ansteht. Demzufolge sind hier die Erkenntnisse aus der Ist-Analyse relevant.

Der Funktionsumfang einer **Workflow-Komponente für Kontroll- und Freigabemechanismen** sollte über einen selbständig durchgeführten Funktionstest ermittelt werden. Hierfür ist zunächst der Freigabeprozess für Webinhalte zu definieren. Dieser Prozess muss anschließend mit dem Workflow-Modul automatisierbar sein. Beim Funktionstest ist zudem zu überprüfen, ob eine **Vorschaufunktion** sowie eine Möglichkeit zum **Publizieren** zur Verfügung steht.

Die Workflow-Komponente muss neben Mechanismen zur Kontrolle und Freigabe auch die Möglichkeit bieten, Webinhalte **automatisch zu archivieren** und den Redakteur **automatisch auf eine anstehende Aktualisierung** hinzuweisen. Ob sie dazu fähig ist, muss ebenfalls über einen manuellen Funktionstest verifiziert werden.

Eine Kompatibilität der integrierten **Suchfunktion** mit den vorhandenen Speichermechanismen (vgl. Ist-Analyse) geht aus den Herstellerspezifikationen des WCMS hervor. Gleiches gilt für die **Versionsverwaltungskomponente**. Sie muss die unter Abschnitt 4.3.6.2.6 definierten Funktionen unterstützten.

Zur Soll-Konzeption bzgl. der **Rollen- und Rechteverwaltung** ist die Anwendungsdomäne genau zu analysieren, möglichst im Rahmen der Anforderungserhebung mit den Redakteuren (vgl. Abschnitt 4.3.6.3.1), erweitert um Administratoren des jetzigen Webauftritts und des WCMS. Dabei sind mindestens die folgenden Fragen zu stellen:

- Ist zwischen Redakteur und Administrator zu unterscheiden?
- Ist zwischen Administrator und Prüfer/Publizierer zu differenzieren?
- Soll das WCMS mandantenfähig sein?
- Sind Administratoren detaillierter zu unterscheiden? Sollen beispielsweise ein globaler Systemadministrator und lokale Administratoren für Webauftritte von Mandanten existieren?
- Soll der Webauftritt personalisierte Inhalte anbieten? Wenn ja, dann ist zwischen Gast und autorisiertem Nutzer zu unterscheiden.
- Ist es notwendig, die Rechte der autorisierten Nutzer weiter zu untergliedern? Z.B. wenn nur einigen angemeldeten Nutzern das Editieren von Wikis erlaubt ist.

Weitere potentielle Fragen ergeben sich aus einer detaillierten Analyse der Aufbau- und Ablauforganisation betroffener Abteilungen bzw. Behörden. Wird z.B. der Webauftritt von nur einer Person betreut, muss nicht zwischen Administrator und Redakteur unterschieden werden. Ob das hier entstehende Rollenmodell durch die Rollen- und Rechteverwaltung des WCMS abbildbar und ob es **übersichtlich und einfach bedienbar** ist, ergibt sich aus einem prototypischen Betrieb des WCMS. Hierbei kann auch das Vorhandensein einer **Vererbungsfunktion** für Rollen überprüft werden.

Das Bestimmen eines optimalen **Erweiterungsmechanismuses** ist kaum möglich. Es empfiehtl sich daher eine Analyse von Existenz, Güte und Umfang der **API** des WCMS[219]. Dabei kann gleichzeitig der Umfang und die Qualität der verfügbaren Erweiterungen überprüft werden[220].

[219] z.B. http://api.typo3.org/, abgerufen: 10.08.2011

[220] z.B. http://wordpress.org/extend/Plug-Ins/jetpack/. Rating der Nutzer, Anzahl Downloads und Datum der letzten Aktualisierung. Abgerufen: 10.08.2011

Der aktuell relevante Funktionsumfangs des **Sicherheitsmoduls** (vgl. Abschnitt 4.3.6.2.9) ergibt sich aus Analysen zu gängigen Sicherheitslücken in Web-Anwendungen. Dort sind i.d.R. Gegenmaßnahmen beschrieben, auf die das WCMS hinweisen sollte (vgl. (CWE11), (The10)). Ob dies der Fall ist, lässt sich nur über einen Funktionstest detailliert bestimmen. Dabei ist auch die **Administrationsoberfläche** auf ihren Funktionsumfang zu prüfen. Hier ist es wichtig, dass komfortabel und detailliert Optionen ein- bzw. ausgeschaltet werden können und auch dass ein einfaches Integrieren von Erweiterungen ermöglicht wird.

Neben den Sicherheitsmechanismen stellt die **Migrationsunterstützung** ein zentrales Bewertungskriterium dar. Wie diese konkret aussehen soll, ist nicht pauschal definierbar, weil unterschiedliche WCMS i.d.R. ihre Daten auch verschieden abspeichern. In der Folge existieren mit sehr großer Wahrscheinlichkeit zwei unterschiedliche Datenschemata – das des momentan eingesetzten und das des künftigen WCMS. Um das alte in das neue Schema zu überführen, sind Methoden der Schematransformation bzw. -Integration oder ETL-Prozesse notwendig. Das konkrete Vorgehen hängt von der jeweiligen Situation ab und kann folglich nicht allgemein beschrieben werden. Stets von Vorteil sind Anleitungen, Skripte o.ä., die für ähnliche Schematransformationen geschrieben wurden. Sie können entweder unmittelbar oder zumindest als Anhaltspunkt verwendet werden. Folglich sind eine Internet-Recherche oder eine Hinzuziehung von Spezialisten ratsam. ETL-Werkzeuge (Extraktion, Transformation, Laden) können u.a. dazu verwendet werden, Daten aus mehreren ggf. unterschiedlich strukturierten Datenquellen in einer Zieldatenbank zu vereinigen[221]

Bisher wurden primär allgemeine Anforderungen an WCMS beschrieben, die domänenübergreifend gelten. In bestimmten Einsatzgebieten können zusätzlich dazu noch diverse weitere Aspekte relevant werden. Es ist beispielsweise denkbar, dass für ausländische Zielgruppen mehrsprachige Webseiten zu erstellen sind oder dass der Webauftritt auf kommunikative Features wie Soziale Netzwerke setzt. Beide Aspekte müssen ggf. in der Bewertung der Alternativen berücksichtigt werden.

Auch bei der Erstellung von Webinhalten können diverse weitere Aspekte eine Rolle spielen. Viele WCMS bieten z.B. die Möglichkeit, kollaborativ Webinhalte zu erstellen, etwa durch einen in die Editoren integrierten (Video-) Chat.

#### 4.3.6.4 Aktuell relevante Alternativen

SAGA schreibt bei Fachverfahren die Analyse verfügbarer EFA-Angebote vor (Die11b). Dazu zählt auch der proprietäre Government Site Builder, der ein Einer-für-Alle-Angebot bei den WCMS darstellt[222]. Die gängisten Open-Source-Alternativen sind Drupal, Typo3, Joomla und WordPress.

#### 4.3.6.5 Migrations-Checkliste

Das sequenzielle Durchlaufen der nachfolgenden Checkliste stellt sicher, dass alle relevanten Aspekte bei der Migration eines WCMS berücksichtigt werden. Die jeweils letzte Zeile zeigt, wie zur Bewertung des Kriteriums vorzugehen ist.

##### 4.3.6.5.1 Ist-Analyse

1. Vorhandene Dateiformate, Skript- und Programmiersprachen von Webinhalten bestimmen. Befragung der Redakteure und Administratoren, Analyse der Server-Log-Files.
2. Datenmodelle des Archivsystem-Datenspeicher bzw. des WCMS-Datenspeicher erstellen. Befragung der Rechenzentrums-, WCMS- bzw. Archivsystemadministratoren.

[221] vgl. http://de.wikipedia.org/wiki/ETL-Prozess, abgerufen: 10.08.2011
[222] http://www.cio.bund.de/DE/IT-Angebot/Basis-IT/GSB/gsb_node.html, abgerufen: 24.10.2011

#### 4.3.6.5.2 Soll-Konzeption

1. Analyse des Inhalts- und Struktur- bzw. Layout-Editors
   Welche von SAGA empfohlenen bzw. vorhandenen Datenformate müssen unterstützt werden? Bieten die Editoren einen Assistenten, der die Anforderungen der BITV zu erfüllen hilft? Welche Funktionen zur Suchmaschinenoptimierung bieten die Editoren? Welche Skriptsprachen können verwendet werden? Welche Dateiformate sind importierbar?
   Anforderungsanalyse mit Redakteuren bzgl. funktionaler Anforderungen an die Editoren.

2. Speichermöglichkeit bzw. eine Anbindung an eine vorhandene Speichermöglichkeit
   Wie und worauf sollen Dateien künftig gespeichert bzw. archiviert werden?
   Kommunikation mit zuständigen Fachkräften.

3. Versionsverwaltung
   Können Dokumente versioniert und dabei Metadaten (Ersteller, Datum) festgehalten werden? Ist ein Vergleich von konfliktären Dokumenten möglich? Ist ein Abzweigen von Dokumenten möglich? Ist ein systemweites Umbenennen von Dateien möglich?
   Anforderungsanalyse mit Redakteuren bzgl. weiterer funktionaler Anforderungen an die Versionsverwaltung

4. Workflow-Komponente für Kontroll- und Freigabemechanismen
   Wie sieht der Kontroll- und Freigabeprozess der Zieldomäne aus? Kann er mit der Workflow-Komponente abgebildet werden?
   Anforderungsanalyse mit Prozessverantwortlichen

5. Vorschaufunktion
   Kann dem Anwender eine unveröffentlichte Vorschau angezeigt werden?

6. Automatisches Archivieren bzw. automatische Aktualisierungsaufforderung
   Kann die Workflow-Komponente derartige Prozesse automatisieren?
   Funktionstest mit Hilfe eines Prototypen.

7. Integration mit Archivsystem

8. Suchfunktion
   Ist die Suchfunktion mit der des Archivsystems integrierbar? Können aktuell publizierte Webinhalte durchsucht werden?
   Funktionstest mit Hilfe eines Prototypen.

9. Rollen- und Rechteverwaltung
   Kann das Rechtemodell umgesetzt werden? Ist die Vererbung von Rollen möglich? Ist die Administration übersichtlich?
   Bestimmung des Rechtemodells durch Kommunikation mit relevanten Abteilungen und Funktionstest mit Hilfe eines Prototypen.

10. Erweiterbarkeit
    Bietet das WCMS eine API für den Zugriff auf Grundfunktionen? Ist diese API gut dokumentiert und frei zugänglich? Sind ausreichend Module in guter Qualität vorhanden?

11. Sicherheitsmodul
    Werden erstellte Webinhalte auf Sicherheitslücken überprüft? Werden dabei aktuelle Sicherheitslücken berücksichtigt?
    Analyse aktueller Sicherheitsstudien und Funktionstest mit Hilfe eines Prototypen.

12. Administrationsoberfläche
    Was ist zu administrieren? Sind alle Einstellungen leicht verständlich und komfortabel erreichbar?

13. Migrationsunterstützung
    Existieren Skripte, Beschreibungen oder ETL-Prozesse für die notwendige Datenmigration?
    Internet-Recherche und Experteninterviews.

### 4.3.7 PDF-Reader und -Authoring

Der Umgang mit Dokumenten im Portable Document Format (PDF) ist im Büro-Alltag eine Selbstverständlichkeit geworden. Die Unabhängigkeit dieses Formats von bestimmten Plattformen, Programmen und Hardware führte zu einer hohen Akzeptanz und weltweiter Verbreitung. In SAGA ist PDF als verbindlicher Standard für den Informationsaustausch von Textdokumenten, Tabellen und Präsentationen definiert.

#### 4.3.7.1 Einleitung

Adobe Systems Inc. als Urheber des Formats trat 2001 die Rechte an einigen Teilen an die International Organization for Standardization (ISO) ab, die darauf basierend den Standard PDF/X für Druckvorlagen als ISO 15930-1:2001 normierte. 2005 wurde unter dem Bezeichner ISO 19005-1:2005 PDF/A auf der Basis von PDF 1.4 für die Langzeitarchivierung von Dokumenten standardisiert, und 2008 veröffentlichte die ISO unter der Nummer 32000-1:2008 einen vollumfänglichen Standard für portable Dokumente in der Version PDF 1.7. Auf diesem basiert auch die Aktualisierung des PDF/A-Standards, die 2011 als ISO 19005-2:2011 veröffentlicht wurde.

Der PDF/A-Standard verbietet vor dem Hintergrund der Langzeitarchivierung bestimmte Merkmale des normalen PDF-Standards wie die Verschlüsselung und dynamische Inhalte, z.B. Skripte oder Audio- und Videodaten. Andererseits verlangt er das Vorhandensein ansonsten optionaler Merkmale wie bestimmte Metadaten oder die Einbettung aller verwendeten Schriften. Eine elektronische Signatur ist in beiden Standard-Varianten möglich. PDF-Dateien können generell in PDF/A-Dokumente gewandelt werden; für PDF/A unzulässige Bestandteile werden je nach Werkzeug bemängelt oder ignoriert. PDF/A-Dokumente wiederum können von allen Standard-konformen PDF-Betrachtern dargestellt werden.

Durch die offene Standardisierung dieser Formate nimmt die Zahl unterstützender Software-Produkte stetig zu. Im Bereich der Office-Suiten gehört das Erstellen von PDF-Dokumenten heute zur Standard-Funktionalität (siehe 4.3.4), und das Darstellen solcher Dokumente ist längst nicht mehr auf den Adobe Acrobat Reader eingeschränkt. Allerdings bestehen zwischen den verschiedenen Werkzeugen zum Erstellen, Bearbeiten und Darstellen von PDF-Dokumenten Unterschiede, die bei der Beschaffung geeigneter Software berücksichtigt werden müssen.

#### 4.3.7.2 Kriterienkatalog

Neben der Betrachtung der jeweiligen **Lizenzen** und der unterstützten **Plattformen** muss beim Erstellen von PDF-Dokumenten geprüft werden, welche **Versionen des Standards** unterstützt werden, ob interaktive **Formulare** erstellt und Dokumente mit einer digitalen **Signatur** versehen werden können. Zudem müssen gem. BITV zur Veröffentlichung bestimmte Dokumente **barrierefrei** erstellt werden können, beispielsweise durch Tags oder Farbräume mit starker Konstrastierungsmöglichkeit.

Beim Umgang mit bestehenden PDF-Dokumenten sollte die **Darstellung** an die Bedürfnisse angepasst (z.B. Drehen, Vergrößern, Doppelseiten-Ansicht), Dokumente **durchsucht**, Gliederungen und Verweise zur **schnellen Navigation** im Dokument genutzt und **Kommentare, Korrekturen** u.ä. geeignet dargestellt werden können.

Bei der Bearbeitung bestehender PDF-Dokumente sollte das Anbringen von **Kommentaren** sowie die **Kennzeichnung** und **Korrektur** bestimmter Passagen samt digitaler **Signatur** der Änderungen möglich sein.

Die im PDF-Standard vorgesehenen Möglichkeiten zum Schutz eines Dokuments vor ungewolltem Gebrauch umfassen im Wesentlichen die Verschlüsselung des gesamten Dokuments sowie das Verhindern von Druck und Inhalts-Extraktion. Letztere beide lassen sich allerdings problemlos beispielsweise durch Bildschirmdruck (Screenshot) und OCR-Software umgehen, und auch die PDF-eigene Verschlüsselung bietet keinen ausreichenden Schutz vor unbefugtem Zugang. PDF-Dokumente sollten daher generell ohne diese trügerischen Schutzmechanismen erstellt und ausgetauscht werden.

Schutzbedürftige Informationen von und für Behörden unterliegen ohnehin den Bestimmungen des Geheimschutzes, und der Umgang mit elektronischen Dokumenten ist im Geheimschutzhandbuch umfänglich geregelt. Daher wird bei der Betrachtung von PDF-Werkzeugen nicht weiter auf Format-spezifische Sicherheitsaspekte eingegangen.

Beachtet werden sollte hingegen, welche Informationen über die Metadaten eines Dokuments oder in Form unsichtbarer oder geschwärzter Passagen weitergegeben werden. Die Preisgabe des letzten Änderungsdatums oder der Autoren kann ebenso unerwünscht sein wie die des Erstellungswerkzeugs, woraus Angreifer ggf. Rückschlüsse auf bestehende Sicherheitslücken ziehen können. Mit Sicherheit unerwünscht ist das Auffinden und Sichtbarmachen geschwärzter Passagen durch eine einfache Textsuche. Daher sollte ein PDF-Betrachter die **Metadaten anzeigen** und ein PDF-Ersteller deren **Anpassung** und die **Bereinigung** eines Dokuments von versteckten Inhalten ermöglichen. Einen guten Überblick über entsprechende Werkzeuge und die Fähigkeiten der meistverwendeten PDF-Erstellungshilfen liefert (Tri11).

#### 4.3.7.3 Methodik

##### 4.3.7.3.1 Ist-Analyse

Im Rahmen der Ist-Analyse gilt es zu untersuchen,

- mit welchen Werkzeugen
- in welchen Versionen
- für welche Zwecke

derzeit PDF-Dokumente erstellt werden. Dies umfasst die Veröffentlichung von Informationen auf eigenen Webseiten, den Informationsaustausch mit anderen Behörden, Wirtschaftsbeteiligten und Bürgern (Externen), die Bereitstellung von elektronischen Formularen und die Archivierung von Dokumenten. Dabei sollte geprüft werden, ob die erstellten Dokumente bereits durch eine einfache, fortgeschrittene oder qualifizierte elektronische Signatur mit einem dem Signaturgesetz (SigG) entsprechenden Rechtscharakter versehen werden. Zudem gilt es herauszufinden, welche Schutzmerkmale und Gestaltungsoptionen derzeit genutzt werden und ob die Erstellung von PDF-Dokumenten in definierte Arbeitsprozesse eingebunden ist.

Beim Empfang von PDF-Dokumenten sollte geprüft werden, mit welchen Werkzeugen diese derzeit gelesen werden, ob aktuelle Versionen des Standards geöffnet, ggf. vorhandene elektronische Signaturen sicher erkannt und Anmerkungen und Korrekturen geeignet und vollständig dargestellt werden können. Auch gilt es zu ermitteln, ob empfangene PDF-Dokumente korrigiert oder mit Anmerkungen versehen werden müssen und mit welchen Werkzeugen dies derzeit umgesetzt wird.

##### 4.3.7.3.2 Soll-Konzeption

Für den künftigen Einsatz von PDF-Dokumenten gilt es zu ermitteln, in welchen Bereichen derzeit Dokumente in bearbeitbaren Formaten versandt und empfangen werden und dies auf (weitgehend) unveränderbare PDF-Dokumente umgestellt werden soll. Dazu sollten mindestens die Bereiche einer Behörde befragt werden, die im Informationsaustausch mit Externen stehen. Bei der Befragung sollte ermittelt werden, wie die Erstellung und Archivierung von PDF-Dokumenten optimal in den Arbeitsablauf integriert werden kann, welche Teilschritte dem einzelnen Anwender überlassen bleiben sollen und welche zentral konfiguriert oder automatisiert werden können. Daraus sollte sich der Bedarf an Werkzeugen zur Erstellung von PDF-Dokumenten in den Varianten Standard und Langzeitarchivierung ergeben. Außerdem sollte daraus hervorgehen, inwieweit die Fähigkeit zu Kommentaren und Änderungen sowie zur gewünschten elektronischen Signatur hergestellt oder erweitert werden sollte. Der Bedarf an solchen Werkzeugen sollte zudem unterschieden werden zwischen lokaler Installation je Anwender und zentraler Installation für die automatisierte Erstellung.

Eingehender Schriftverkehr sollte hinsichtlich der Menge und Komplexität analysiert und dahingehend geprüft werden, ob rechtlich relevante schriftliche und elektronische Dokumente automatisiert in das Format PDF/A überführt und geeignet signiert werden sollten. Sich anschließende elektronische Arbeitsprozesse sollten auf ihre Eignung im Umgang mit signierten PDF/A-Dokumenten überprüft und ggf. erweitert oder migriert werden. Zudem sollte die automatische PDF/A-Erstellung von Papier-Dokumenten mit Werkzeugen zur Optical Character Recognition (OCR) kombiniert werden, die eine Volltextsuche im jeweiligen Inhalt ermöglichen und Metadaten wie Datum, Adressat oder Absender erkennen und im PDF/A-Dokument ablegen können.

#### 4.3.7.4 Betrachtete Alternativen

Betrachtet werden Software-Lösungen zum Erstellen, Darstellen und Bearbeiten von PDF-Dokumenten am Arbeitsplatz. In Abschnitt 4.3.4 wurde für die dort betrachteten Office-Suiten bereits dargestellt, inwieweit die Erstellung von PDF-Dokumenten unterstützt wird. Die Darstellung von PDF-Dokumenten und das Einbringen von Kommentaren o.ä. liegt außerhalb deren Funktionalität, sie werden daher hier nicht erneut betrachtet.

Angesichts der Vielzahl an Lösungen im kommerziellen und OSS-Bereich und des Fehlens belastbarer Aussagen zu deren Verbreitung werden beispielhafte Lösungen betrachtet, die jeweilige Schwerpunkte im Umgang mit PDF-Dokumenten repräsentieren.

Für die Erstellung von PDF-Dokumenten werden folgende Lösungen betrachtet:

- Adobe Acrobat Pro als Lösung des Marktführers,
- Nuance PDF Converter als in Behörden verbreiteter proprietärer Alternative,
- PDFCreator als verbreiteter OSS-Lösung zur PDF-Erstellung via Pseudodrucker.

Für die Betrachtung und Überarbeitung von PDF-Dokumenten werden folgende Lösungen betrachtet:

- Adobe Acrobat Reader als Lösung des Marktführers,
- PDF-XChange Viewer als in Behörden verbreiteter proprietärer Alternative,
- Evince als verbreiteter OSS-Lösung.

Die massenhafte automatisierte Erstellung von PDF/A-Dokumenten durch Dokumentenscanner liegt aufgrund der zu betrachtenden Hardware und darauf abgestimmter Software-Komponenten außerhalb des Spektrums des Migrationsleitfadens. Gleichwohl sollten solche Lösungen in eine ganzheitliche IT-Strategie einfließen und darauf geprüft werden, ob sie die o.g. Kriterien erfüllen.

#### 4.3.7.5 Bewertung

##### 4.3.7.5.1 PDF-Ersteller

Adobe Acrobat[223] ist unter wechselndem Produktnamen seit der Einführung von PDF die Referenzlösung zur Erstellung, Bearbeitung und Darstellung von PDF-Dokumenten und erfüllt mit seinen verschiedenen Komponenten sämtliche Kriterien zur Erstellung, Betrachtung und Bearbeitung von PDF-Dokumenten. Adobe Acrobat wird in verschiedenen Editionen für die Plattformen Windows und MacOS X angeboten, die Beschaffung ist allerdings mit recht hohen Lizenzkosten verbunden. Dafür bringt der Acrobat neben der Unterstützung sämtlicher ISO-normierter PDF-Standards[224] auch Werkzeuge zur Validierung von Dokumenten gegen diese Standards mit und kann PDF-Dokumente miteinander vergleichen. Adobe Acrobat kann Kommentare an PDF-Dokumenten in die Änderungsverfolgung von Microsoft Word übernehmen und Rückläufer von PDF-Formularen auswerten. Außerdem ist der Acrobat in der Lage, sämtliche versteckten oder geschwärzten Inhalte aufzuspüren und das Dokument davon zu bereinigen.

[223] http://www.adobe.com/de/products/acrobatpro.html
[224] Das sind derzeit PDF 1.7, PDF/A in den Varianten 1a, 1b, 2a und 2b, PDF/X und PDF/E.

Im Bereich der PDF-Erstellung gibt es zum Adobe Acrobat kein vergleichbares OSS-Produkt, wohl aber einige proprietäre Alternativen wie Foxit PhantomPDF[225], Nuance PDF Converter[226] oder PDF-XChange PRO von Tracker Software[227] mit ähnlichem Funktionsumfang, aber deutlich geringeren Lizenzkosten. Der beispielhaft untersuchte PDF Converter von Nuance unterstützt mit PDF 1.7 und PDF/A-1b die derzeit wichtigsten ISO-normierten Standards für den Behördenbetrieb und bietet umfassende Erstellungs- und Korrekturwerkzeuge, das Erstellen von PDF-Formularen und die Einbindung digitaler Signaturen. PDF-Dokumente werden mit ggf. vorhandenen Überarbeitungsmerkmalen angezeigt. Dokumente können verglichen, Metadaten korrigiert, versteckte Inhalte aufgespürt und Bilddaten per OCR ggf. in Text gewandelt werden. Wie die anderen genannten Alternativen ist der PDF Converter auf Windows-Plattformen beschränkt.

Der PDFCreator dient unter Windows als Pseudodrucker zur Erstellung von PDF-Dokumenten. Er wird im System als weiterer lokaler Drucker installiert und kann dann von allen zum Ausdruck fähigen Programmen verwendet werden. Per Optionendialog können diverse Voreinstellungen definiert werden, beispielsweise eine bestimmte PDF-Version[228] oder die automatische elektronische Signierung mit einer entsprechenden Zertifikatsdatei. Beim Ausdruck können die Optionen gezielt angepasst werden; alternativ kann das Speichern automatisiert und Regeln für Format, Ablage und Dateinamenserstellung der resultierenden PDF-Dokumente definiert werden. Der PDFCreator steht unter der GPL als OSS frei zur Verfügung. Die beiliegende Toolbar zur bequemen Erstellung von PDFs von besuchten Internetseiten dürfte allerdings im Behördenbetrieb keine Vorteile bringen und sollte daher bei der Installation abgewählt werden.

Die nachfolgende Tabelle bietet eine Übersicht über die Fähigkeiten der einzelnen Werkzeuge zur Erstellung und Bearbeitung von PDF-Dokumenten.

Tabelle 4.15: Vergleich PDF-Erstellung

| Produkt | Adobe Acrobat | PDF Converter | PDFCreator |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | – | – | ✓ |
| Lizenzkosten | pro Installation, Volumenlizenzen | pro Installation, Volumenlizenzen | – |
| Unterstützte Plattformen (Windows XP / 7 / Linux / MacOS X) | ✓/✓/–/✓ | ✓/✓/–/– | ✓/✓/–/– |
| Unterstützte PDF-Versionen 1.4 / 1.7 / PDF/A | ✓/✓/✓ | ✓/✓/✓ | ✓/–/✓ |
| **PDF-Erstellung** | | | |
| Formular-Erstellung | ✓ | ✓ | – |
| Digitale Signatur | ✓ | ✓ | ✓ |
| Barrierefreiheit | ✓ | ✓ | – |
| Pseudodrucker[229] | ✓ | ✓ | ✓ |
| **PDF-Darstellung** | | | |
| Metadaten anzeigen | ✓ | ✓ | – |

[225] http://www.foxitsoftware.com/products/phantomPDF/
[226] http://www.nuance.de/products/pdf-converter-professional7/index.htm
[227] http://www.tracker-software.com/product/pdf-xchange-pro
[228] Zur Auswahl stehen die Varianten PDF v1.2 - v1.5 und PDF/A-1b
[229] Erstellung von PDF-Dokumenten über Druck-Funktionalität

| Produkt | Adobe Acrobat | PDF Converter | PDFCreator |
|---|---|---|---|
| Anpassbarkeit<br>Drehen/Vergrößern/Doppelseiten | ✓/✓/✓ | ✓/✓/✓ | –/–/– |
| Volltextsuche / Mustersuche | ✓/✓ | ✓/✓ | –/– |
| Navigation<br>Gliederungen/Verweise/Seitenvorschau | ✓/✓/✓ | ✓/✓/✓ | – |
| Anzeige Überarbeitung<br>Kommentar/Korrektur/Hervorhebung | ✓/✓/✓ | ✓/✓/✓ | –/–/– |
| **PDF-Bearbeitung** | | | |
| Metadaten korrigieren | ✓ | ✓ | – |
| Dokument bereinigen | ✓[230] | ✓[231] | – |
| Kommentare | ✓ | ✓ | – |
| Korrekturen | ✓ | ✓ | – |
| Hervorhebungen | ✓ | ✓ | – |
| Formulardaten speichern | ✓ | ✓ | – |
| Änderungen signieren | ✓ | ✓ | – |

#### 4.3.7.5.2 PDF-Betrachter

Evince[232] ist ein schlankes OSS-Produkt zur Darstellung und Kommentierung von PDF-Dokumenten. Es bietet eine Volltextsuche, eine Ansicht für die Metadaten und verschiedene Darstellungsoptionen wie Präsentationsmodus, stufenlose Vergrößerung oder Farbinvertierung. Die Kommentierungsmöglichkeiten beschränken sich auf die Platzierung eines wählbaren Kommentarzeichens im Text und der Eingabe des Kommentars. Das Löschen eines Kommentars ist ebenso wenig möglich wie Unterstreichungen oder Korrekturen am Text. Von anderer Software eingebrachte Kommentare werden korrekt wiedergegeben; Korrekturen werden zwar erkannt, aber nur als Symbole im Text ohne Inhalt dargestellt. Evince ist unter der GPL v2 verfügbar für die Plattformen Windows und Linux.

Evince ist kein vollständiger Ersatz für den Adobe Acrobat Reader und bietet bei den Überarbeitungsfunktionen lediglich rudimentäre Unterstützung. Das Darstellen und Drucken von PDF-Dokumenten ist allerdings genügend ausgereift und für den Wirkbetrieb geeignet. Alternative OSS-Produkte zur Darstellung von PDF-Dokumenten gibt es einige, u.a. Sumatra PDF und Okular; die FSFE pflegt eine Liste mit freien PDF-Betrachtern[233].

Als Freeware (siehe 2.7) stehen weitere PDF-Betrachter zur Verfügung, neben dem weit verbreiteten Adobe Acrobat Reader[234] beispielsweise der Foxit Reader[235] oder der PDF-XChange Viewer[236].

Der Acrobat Reader bringt erwartungsgemäß den größten Funktionsumfang mit und erweist sich als passendes Gegenstück zum PDF-Ersteller aus demselben Hause. Im Gegensatz zu Letzterem läuft der Acrobat Reader auch unter Linux und bietet alle unter Evince aufgeführten Merkmale. Zusätzlich werden

[230] Teilweise durch „Ausgeblendete Informationen entfernen“, vollständig durch „Dokument bereinigen“.
[231] Teilweise durch „Dokument prüfen“, Rest manuell per Navigationsleiste
[232] http://projects.gnome.org/evince/
[233] http://pdfreaders.org/
[234] http://www.adobe.com/products/reader/
[235] http://www.foxitsoftware.com/Secure_PDF_Reader/
[236] http://www.tracker-software.com/product/pdf-xchange-viewer

sämtliche Überarbeitungsfunktionen vollständig unterstützt, der Reader kann Formulardaten speichern, Änderungen digital signieren lassen und nach Textmustern suchen.

Der PDF-XChange Viewer bietet unter Windows und per Wine[237] auch unter Linux ausgereifte Überarbeitungsfunktionen und hinsichtlich der betrachteten Funktionalität nahezu denselben Umfang wie die Freeware des Marktführers. Dazu gehören umfassende Bearbeitungsmöglichkeiten, eine Volltext- und Wortkombinationssuche sowie umfassende Einblicke in die Metadaten. Das Signieren von Dokumenten ist allerdings auf die mit Lizenzkosten verbundene Pro-Version beschränkt.

Tabelle 4.16: Vergleich PDF-Anzeige

| Produkt | Acrobat Reader | Evince | PDF-XChange Viewer |
|---|---|---|---|
| **Metainformationen** | | | |
| OSS-Lizenz | – | ✓ | – |
| Lizenzkosten | – | – | – |
| Unterstützte Plattformen<br>(Windows XP / 7 / Linux / MacOS X) | ✓/✓/✓/✓ | ✓/✓/✓/✓ | ✓/✓/✓[238]/– |
| Unterstützte PDF-Versionen<br>1.4 / 1.7 / PDF/A | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| **PDF-Darstellung** | | | |
| Metadaten anzeigen | ✓ | ✓ | ✓ |
| Anpassbarkeit<br>Drehen/Vergrößern/Doppelseiten | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| Volltextsuche / Mustersuche | ✓/✓ | ✓/– | ✓/✓[239] |
| Navigation<br>Gliederungen/Verweise/Seitenvorschau | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| Anzeige Überarbeitung<br>Kommentar/Korrektur/Hervorhebung | ✓/✓/✓ | ✓/–/– | ✓/✓/✓ |
| **PDF-Bearbeitung** | | | |
| Metadaten korrigieren | ✓ | – | ✓ |
| Kommentare | ✓ | ✓ | ✓ |
| Korrekturen | ✓ | – | ✓ |
| Hervorhebungen | ✓ | – | ✓ |
| Formulardaten speichern | ✓ | – | ✓ |
| Änderungen signieren | ✓ | – | ✓[240] |

[237] Wine ist ein Emulator für Windows-Programme unter Linux.
[238] Läuft im Emulator Wine auch unter Linux.
[239] Nur Groß-/Kleinschreibung und Wortkombinationen, keine regulären Ausdrücke
[240] Nur mit der PRO-Version möglich, für die Lizenzkosten anfallen.

#### 4.3.7.6 Empfehlungen

Das Darstellen von PDF-Dokumenten ist mit vielen verschiedenen Werkzeugen möglich. Solange keine Kommentierungs- oder Überarbeitungsfunktionen benötigt werden, ist man in der Wahl des Werkzeugs frei. Werden PDF-Dokumente öffentlich bereitgestellt, sollten Behörden fairerweise zu deren Betrachtung nicht mehr ausschließlich den Adobe Acrobat Reader empfehlen, sondern beispielsweise die von der FSFE bereitgestellten HTML-Bausteine[241] zum Download alternativer PDF-Betrachter in ihre Seiten aufnehmen.

Sind Überarbeitungsfunktionen notwendig, kann derzeit lediglich zwischen verschiedenen proprietären Produkten gewählt werden. Die aktuellen Fähigkeiten von Evince und vergleichbaren OSS-Alternativen sind unzureichend. Hier wäre ein behördliches Engagement zur diesbezüglichen Weiterentwicklung vorhandener OSS-Alternativen sinnvoll, um nicht in ungewollter Abhängigkeit von einzelnen Anbietern proprietärer Produkte zu verharren.

Zur Erstellung von PDF-Dokumenten eignet sich der Adobe Acrobat angesichts seiner enormen Funktionsfülle in jedem Fall. Doch auch alternative PDF-Erstellungswerkzeuge wie der betrachtete PDF Converter weisen vielfach durchaus vergleichbare Fähigkeiten auf. Bei der Veröffentlichung von PDF-Dokumenten ist darauf zu achten, dass nicht zur Veröffentlichung bestimmte Teile zuvor entfernt wurden. Die umfassendste Unterstützung hierbei leistet der Adobe Acrobat, gefolgt vom Nuance PDF Converter. Bei allen Alternativen sollte geprüft werden, welche der gebotenen Möglichkeiten tatsächlich benötigt werden und die Lizenzkosten rechtfertigen. Den betrachteten Mindestumfang deckt der PDF Converter praktisch ebenso gut ab wie der Adobe Acrobat, ist deutlich günstiger und daher zu empfehlen.

Die Fähigkeit von Adobe Acrobat zur Übernahme von Kommentaren an PDF-Dokumenten in die Änderungsverfolgung von Microsoft Word ist zwar bemerkenswert, aber ohne gleichartige Unterstützung des ODF-Standards eher das Gegenteil des Erwünschten. Denn diese einseitige Ausrichtung des einen Marktführers am Produkt des anderen führt nicht zur Wahlfreiheit zwischen den besten Lösungen des jeweiligen Gebiets, sondern zur Festigung unerwünschter Monopole. Ebenso bemerkenswert wie fraglich ist die Fähigkeit verschiedener Produkte zur Erstellung von PDF-Formularen samt darauf basierender Auswertung von Rückläufern, da eine Web-gestützte Datenerhebung bei ähnlichem Erstellungsaufwand eine unmittelbare Auswertbarkeit und mit geringem Zusatzaufwand eine sichere Kommunikationsverbindung bietet.

Die Plattformen Linux und MacOS X bieten jeweils generische Pseudodrucker zur Erstellung einfacher PDF-Dokumente, erreichbar beispielsweise unter Linux im Druck-Dialog als „In Datei drucken“. Diese Pseudodrucker bieten allen Anwendungen mit Druckfunktion grundlegende Möglichkeiten zur PDF-Erstellung. Zwar decken sie jeweils nur wenige Möglichkeiten des Standards ab, doch diese genügen durchweg zur Erstellung einfacher PDF-Dokumente. Solange keine weitergehenden Aspekte wie Formularerstellung, Berechtigungen, PDF/A oder die gezielte Beeinflussung von Metadaten notwendig sind, kann auf die Installation spezifischer Lösungen verzichtet werden. Unter Windows bietet sich die Installation des PDFCreator an, der über die Grundfunktionen eines Pseudodruckers hinaus diverse Einstellmöglichkeiten bietet und PDF/A unterstützt.

Für alle Plattformen steht mit OpenOffice eine weitergehende Möglichkeit zur Erstellung solcher Dokumente bereit. OpenOffice bietet die Auswahl zwischen Standard-PDF und PDF/A, das Editieren verschiedener Metadaten in der Quelldatei und deren Übernahme in das PDF-Dokument sowie verschiedene Optionen zur weiteren Gestaltung wie das Taggen von Strukturelementen als Grundlage für die Barrierefreiheit. Ähnlich weitgehende Optionen stellt auch das Microsoft Office zur Verfügung und kann daher analog zu OpenOffice für die Erstellung von PDF-Dokumenten verwendet werden.

[241] http://pdfreaders.org/graphics.de.html

# Kapitel 5

# Zukunftsthemen der IT

Der IT-Bereich ist seit Jahrzehnten im beständigen Fluss, grundlegende Paradigmen ändern sich alle paar Jahre, eine Verstetigung ist nicht abzusehen. Die in diesem Migrationsleitfaden betrachteten Technologiefelder dürften auch in naher Zukunft noch einige Relevanz aufweisen. Allerdings sind Verschiebungen in der Relevanz zwischen den einzelnen Themen zu erwarten.

## 5.1 Cloud Computing

Cloud Computing umschreibt den Ansatz, abstrahierte IT-Infrastrukturen wie Rechenkapazität, Datenspeicher, Netzwerkkapazitäten oder auch fertige Software dynamisch, also an den jeweiligen Bedarf angepasst, über ein Netzwerk zur Verfügung zu stellen. Je nach Angebotsart wird unterschieden zwischen

- der **Public Cloud**, deren Dienste öffentlich angeboten werden,
- der **Private Cloud**, deren Dienste nur innerhalb der eigenen Organisationseinheit angeboten werden, und
- der **Hybrid Cloud**, deren Dienste innerhalb der eigenen und für ausgewählte weitere Organisationseinheiten angeboten werden.

Der IT-Rat hat mit seinen Beschlüssen zum Aufbau der IT-Dienstleistungszentren des Bundes (DLZ-IT) implizit auch die organisatorischen Rahmenbedingungen für eine in der Zukunft denkbare, mit hohem Sicherheitsniveau versehene hybride Bundes-Cloud gelegt. Allerdings bleibt abzuwarten, wann Bundesbehörden von dieser neuen Form von IT-Infrastruktur in größerem Umfang profitieren können. Viele Themen wie die vertragliche Vereinbarung des Leistungsumfangs (SLA) oder die Leistungsabrechnung sind noch ebenso wenig geklärt wie konkrete Angebote aus den Bereichen der Basis- und der Querschnitts-IT.

Die Standardisierung der Cloud-Technologien ist ebenfalls noch im Werden begriffen. Das im Jahr 2009 veröffentlichte *Open Cloud Manifest*[1] führt zwar viele auch namhafte Firmen als „Supporter“, bleibt inhaltlich aber im Ungefähren und hat daher keine größere Bedeutung erlangt. Das IEEE verfolgt seit Mitte 2011 einen eigenen Standardisierungsansatz zur Cloud-Interoperabilität[2], der u.a. Dateiformate und Profile adressiert. Ein weiterer Ansatz zur Interoperabilität im Cloud-Umfeld und der Durchsetzung offener Standards wird von der Open Cloud Initiative[3] verfolgt, die Ihre Vision folgendermaßen beschreibt:

[1] www.opencloudmanifesto.org
[2] http://standards.ieee.org/develop/project/2301.html, siehe auch http://heise.de/-1221583
[3] http://www.opencloudinitiative.org

> „A global cloud of clouds („Intercloud“), interconnected by open standard interfaces exchanging open standard formats („Open Cloud“).“

Welche Standards sich hier entwickeln und durchsetzen, sollte aufmerksam verfolgt werden. Eine frühe Festlegung auf bestimmte Technologien eines Anbieters kann mittelfristig zu beträchtlichen Aufwänden bei der Migration zu einem anderen Anbieter wie der „Bundes-Cloud“ führen. Immerhin existieren im Bereich der Virtualisierung als einer Grundlage für das Cloud Computing erste Standards, siehe 4.2.5.1.6.

## 5.2 Infrastruktur und Desktop-Anwendungen in der Cloud

Der Abschnitt Office-Suiten beschäftigt sich lediglich mit lokal installierten Suiten und lässt die bereits bestehenden Angebote an Cloud-basierten Lösungen außen vor. Der Grund dafür ist, dass derzeit keine mit dem deutschen Datenschutz vollständig vereinbare Form solcher Alternativen angeboten wird. Auch ist noch nicht abzusehen, wie sich der massenhafte Einsatz solcher netzzentrierten Techniken auf den Behördenalltag auswirken wird.

Denkbar ist die Realisierung von Office-Funktionalität über eine hybride Cloud, die von einem DLZ-IT gehostet wird und deutschen Datenschutz-Grundsätzen entspricht. Da die eigenständige Entwicklung einer Office-Suite auf Cloud-Basis unrealistisch ist, sollte beobachtet werden, ob in nächster Zeit Angebote zur Installation solcher Lösungen in einer hybriden Cloud aufkommen. Die Document Foundation plant Entsprechendes auf der Basis von LibreOffice für 2012[4]. Diese Angebote sollten hinsichtlich der unterstützten offenen Standards denselben Prinzipien folgen, wie sie u.a. in 4.3.4.3.4 beschrieben sind.

Als weitere künftige Cloud-Kandidaten kommen beispielsweise Groupware-Lösungen (siehe 4.2.4), Dokumenten Management Systeme (siehe 4.3.5) oder Werkzeuge zur PDF-Erstellung (siehe 4.3.7) in Betracht.

## 5.3 Neue IT-Infrastruktur-Elemente

Die Bundesrepublik Deutschland hat mit der Einführung des neuen elektronischen Personalausweises (ePA) eine Plattform für elektronische Signaturen geschaffen. Zwar ist die Nutzung dieser Möglichkeiten für die Bürger optional, doch kann bei zunehmenden Angeboten zur Verwendung dieser Fähigkeiten auch die Bereitschaft zu deren Einsatz steigen. Der Ausbau von Web-Angeboten des Bundes kann seinen Teil dazu beitragen, wie das Beispiel der Deutschen Rentenversicherung mit dem eService zeigt, über den mit Hilfe des ePA der Stand des eigenen Rentenkontos abgefragt werden kann.

Die anstehende Einführung der DE-Mail trägt ebenfalls dazu bei, dass sich die Voraussetzungen für den elektronischen Rechtsverkehr verbreitern. Bundesbehörden sollten mit dem Beginn deren Wirkbetriebs diese Möglichkeiten annehmen und soweit wie möglich in die Arbeitsabläufe integrieren, damit analog zur elektronischen Signatur über den ePA bald eine kritische Masse von Anwendern erreicht ist, die zum dauerhaften Erfolg dieser Technologie führt.

Ebenfalls mit Interesse verfolgt werden sollten die Entwicklungen rund um elektronische Bezahlsysteme, insbesondere, ob sich offene Standards und freie Implementierungen entwickeln, die von Behörden in entsprechende Angebote integriert werden können.

[4] Siehe http://blog.documentfoundation.org/2011/10/14/libreoffice-conference-announcements/

# Literaturverzeichnis


[B+05] BEER, D. u. a.: Software- und Kriterienkatalog zu RAfEG-Referenzarchitektur für E-Government. In: *Chemnitzer Informatik-Berichte* (2005), Nr. CSR-05-01. http://www.tu-chemnitz.de/informatik/service/if-berichte/pdf/CSR-05-01.pdf. – ISSN 0947–5125

[B+08] BULTERMAN, D. u. a.: *Synchronized Multimedia Integration Language (SMIL 3.0)*. http://www.w3.org/TR/SMIL3/. Version: Dezember 2008

[B+10] BRORS, Dieter u. a.: Offensive 2010. In: *c't* (2010), Nr. 12

[Bar05] BARTLETT, Andrew: *Samba 4 - Active Directory*. Internet. http://www.samba.org/samba/news/articles/abartlet_thesis.pdf. Version: January 2005

[BB11] BAGER, Jo ; BRAUN, Herbert: Browser-Dreikampf. In: *c't* (2011), Nr. 4

[Bec05] BECK, Klaus: *Computervermittelte Kommunikation im Internet*. Oldenbourg Wissenschaftsverlag GmbH, 2005. – ISBN 978–3486578911

[Bes11] BESCHWERDEKAMMER DES EUROPÄISCHEN PATENTAMTS: *Begründung zur Ablehnung des Schutzanspruchs für Amazons One-Klick-Bezahlverfahren*. Internet. http://www.epo.org/law-practice/case-law-appeals/recent/t071244eu1.html. Version: 2011

[BN11] BRORS, Dieter ; NEBELO, Ralf: Kampf der Zwillinge. In: *c't* (2011), Nr. 05

[Bun80] BUNDESMINISTERIUM DER JUSTIZ: *Geheimschutzordnung des Deutschen Bundestages (Anlage 3 der Geschäftsordnung des Deutschen Bundestages, BGBl. I 1980, 1237)*. http://www.gesetze-im-internet.de/btgo1980anl_3/index.html#BJNR012570980BJNE000200311. Version: 1980

[Bun94] BUNDESMINISTERIUM DES INNERN: *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes*. http://www.gesetze-im-internet.de/s_g/index.html#BJNR086700994BJNE001100307. Version: 1994

[Bun02] BUNDESMINISTERIUM DES INNERN: *Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz*. Internet. http://www.gesetze-im-internet.de/bitv_2_0/. Version: April 2002

[Bun05] BUNDESMINISTERIUM DES INNERN: *DOMEA-Konzept Organisationskonzept 2.1*. http://www.verwaltung-innovativ.de/cln_115/nn_684674/SharedDocs/Publikationen/DE/domea__konzept__organisationskonzept__2__1,templateId=raw,property=publicationFile.pdf/domea_konzept_organisationskonzept_2_1.pdf. Version: 2005

[Bun06] BUNDESMINISTERIUM DES INNERN: *Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen - Verschlusssachenanweisung (VS-Anweisung- VSA)*. http://www.

verwaltungsvorschriften-im-internet.de/bsvwvbund_31032006_IS46065201.htm#ivz5. Version: 2006

[Bun08] BUNDESMINISTERIUM DES INNERN: *DOMEA-Anforderungskatalog 2.0*. http://www.verwaltung-innovativ.de/cln_115/nn_684674/SharedDocs/Publikationen/DE/domea__anforderungskatalog__2__0,templateId=raw,property=publicationFile.pdf/domea_anforderungskatalog_2_0.pdf. Version: 2008

[Bun11] BUNDESVERWALTUNGSAMT - BUNDESSTELLE FÜR INFORMATIONSTECHNIK (BIT): *Das Praxishandbuch zum ODF-Beschluss*. http://www.bit.bund.de/. Version: März 2011

[Cab11] CABINET OFFICE, GROSSBRITANNIEN: *Government ICT Strategy*. Internet. http://www.cabinetoffice.gov.uk/content/government-ict-strategy. Version: 2011

[CWE11] CWE COMMUNITY: *2011 CWE/SANS Top 25 Most Dangerous Software Errors*. http://cwe.mitre.org/top25/. Version: 2011

[Der10] DER BEAUFTRAGTE DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK (BFIT): *V-Modell XT Bund*. Internet. http://www.cio.bund.de/DE/Architekturen-und-Standards/V-Modell-XT-Bund/vmodellxt_bund_node.html. Version: 2010

[Die11a] DIE BEAUFTRAGTE DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK (BFIT): *SAGA-Modul Grundlagen, Version de.bund 5.1*. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/saga_modul_grundlagen_de_bund_5_1_0_download.pdf?__blob=publicationFile. Version: 2011

[Die11b] DIE BEAUFTRAGTE DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK (BFIT): *SAGA-Modul Technische Spezifikationen, 5.0*. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/saga_modul_tech_spez_de_bund_5_0_download.pdf?__blob=publicationFile. Version: 2011

[Eur07] EUROPÄISCHER GERICHTSHOF: *Urteil der Großen Kammer, Microsoft vs. EU-Kommission, u.a. Missbrauch einer beherrschenden Stellung durch die Microsoft Corp.* Internet. http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=de&num=79929082T19040201&doc=T&ouvert=T&seance=ARRET. Version: 2007

[Eur10] EUROPÄISCHE KOMMISSION: *Europäischer Interoperabilitätsrahmen (European Interoperability Framework (EIF), Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services'*. http://ec.europa.eu/isa/strategy/doc/annex_ii_eif_en.pdf. Version: Dezember 2010

[EZI09] ECKERT, Dr. Klaus-Peter ; ZIESING, Jan ; ISHIONWU, Ucheoma ; OFFENE KOMMUNIKATIONSSYSTEME FOKUS, Fraunhofer-Institut für (Hrsg.): *Document Interoperability*. Berlin : Fraunhofer Verlag, 2009 http://www.fokus.fraunhofer.de/de/elan/_docs/wp_doc-interop_en_09.pdf. – ISBN 978–3–8396–0047–4

[Fre01] FREYERMUTH, Gundolf S.: Offene Geheimnisse. In: *c't* (2001), Nr. 20. http://heise.de/-285236

[GG05] GROSSKURTH, A. ; GODFREY, M. W.: A Reference Architecture for Web Browsers. In: *Proceedings of the 21st IEEE international conference on software maintenance (ICSM'05)* (2005), Nr. 0

[Hei11] HEISE ZEITSCHRIFTEN VERLAG: *c't kompakt 01/2011 - Linux*. 2011

[Koo07] KOORDINIERUNGS- UND BERATUNGSSTELLE DER BUNDESREGIERUNG FÜR INFORMATIONSTECHNIK IN DER BUNDESVERWALTUNG: *Plattformunabhängigkeit von Fachanwendungen*. Internet. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/plattformunabhaengigkeit_download.pdf?__blob=publicationFile. Version: 2007

[Lam08] LAMPITT, Andrew: *Open-Core Licensing (OCL): Is this Version of the Dual License Open Source Business Model the New Standard?* Internet. http://alampitt.typepad.com/lampitt_or_leave_it/2008/08/open-core-licen.html. Version: 2008

[Mic10a] MICROSOFT: *Configuring and deploying Office 2010*. Internet. http://technet.microsoft.com/en-us/library/cc178982.aspx. Version: 2010

[Mic10b] MICROSOFT: *Document compatibility reference for Excel 2010, PowerPoint 2010, and Word 2010*. Internet. http://technet.microsoft.com/en-us/library/ff871431.aspx. Version: 2010

[Mic10c] MICROSOFT: *Unterschiede zwischen dem OpenDocument-Kalkulationstabellenformat (ODS) und dem Excel-Format (XLSX)*. Internet. http://office.microsoft.com/de-de/excel-help/HA010355787.aspx. Version: 2010

[Mic10d] MICROSOFT: *Unterschiede zwischen dem OpenDocument-Präsentationsformat (ODP) und dem PowerPoint-Format (PPTX)*. Internet. http://office.microsoft.com/de-de/powerpoint-help/HA010355786.aspx. Version: 2010

[Mic10e] MICROSOFT: *Unterschiede zwischen dem OpenDocument-Textformat (ODT) und dem Word-Format (DOCX)*. Internet. http://office.microsoft.com/de-de/starter-help/HA010355788.aspx. Version: 2010

[Mur04] MURPHY, T.: *Research based methods for using powerpoint, animation, and video for instruction*. http://doi.acm.org/10.1145/1027802.1027892. Version: 2004 (SIGUCCS '04)

[NSS10] NSS LABS: *Web Browser Security Socially-Engineered-Malware-Protection*. http://www.nsslabs.com/research/endpoint-security/browser-security/. Version: 2010

[OAS10] OASIS OPEN DOCUMENT FORMAT INTEROPERABILITY AND CONFORMANCE TC: *The State of Interoperability v1.0, Committee Specification 01*. Internet. http://docs.oasis-open.org/oic/StateOfInterop/v1.0/StateOfInterop.pdf. Version: 2010

[Obj10] OBJECT MANAGEMENT GROUP: *OMG Unified Modeling Language Infrastructure*. http://www.omg.org/spec/UML/2.3/Infrastructure/PDF/. Version: 2010

[Ope11] OPENOFFICE.ORG: *OpenOffice.org Administration Guide*. Internet. http://wiki.services.openoffice.org/wiki/Documentation/Administration_Guide. Version: 2011

[Rat08] RAT DER IT-BEAUFTRAGTEN DES BUNDES: *Beschluss Nr. 11/2008: Einführung offener Dokumentenformate in der Bundesverwaltung*. http://www.cio.bund.de/DE/Politische-Aufgaben/Rat-der-IT-Beauftragten/Beschluesse/Tabelleninhalte/beschluss_11_2008.html?nn=2127086. Version: November 2008

[Rat09] RAT DER IT-BEAUFTRAGTEN DES BUNDES: *Rahmenarchitektur IT-Steuerung Bund – Grundlagen, Version 1.0*. Internet. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Architekturen-und-Standards/rahmenarchitektur_itsteuerung_bund_grundlagen_download.pdf?__blob=publicationFile. Version: 2009

[Rog62] ROGERS, E. M.: *Diffusion of innovations*. 5th. New York : Free Press, 1962

[Sie10] SIERING, Peter: Samba 4 kommt. In: *c't* (2010), Nr. 12. http://www.heise.de/ct/artikel/Samba-4-kommt-1003392.html

[The10] THE OPEN WEB APPLICATION SECURITY PROJECT: *The Ten Most Critical Web Application Security Risks*. http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf. Version: 2010

[Tri11] TRINKWALDER, Andrea: Verschwärzt und zugepixelt. In: *c't* (2011), Nr. 18

[WBB10] WEBER, Bernd ; BAUMGARTNER, Patrick ; BRAUN, Oliver: *OSGi für Praktiker*. Carl Hanser Verlag, München, 2010. – ISBN 978–3446420946

[Wei10] WEICHERT, Thilo: *Cloud Computing und Datenschutz*. https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html. Version: Juni 2010

[Win08] WINKELMANN, Axel: *Alltagstauglichkeit von Office-Lösungen – ein Vorgehensmodell zur Auswahl einer Office-Lösung angewendet am Beispiel eines internationalen Logistikunternehmens*. Internet. http://ibis.in.tum.de/mkwi08/01_Alltagstauglichkeit_von_Anwendungssystemen_und_Infrastrukturen/03_Winkelmann.pdf. Version: 2008

[Zan76] ZANGEMEISTER, Christof: *Nutzwertanalyse in der Systemtechnik – Eine Methodik zur multidimensionalen Bewertung und Auswahl von Projektalternativen*. Zangemeister & Partner, 4. Aufl., 1976. – ISBN 3–923264–00–3

# Glossar

**AD** Das **Active Directory (AD)** ist ein Verzeichnisdienst von Microsoft zur Vorhaltung hierarchisch strukturierter Daten zu Benutzern, Diensten und Geräten.. 15, 71, 75, 80, 83, 93, 97, 99, 106

**Add-On** Durch ein Add-On wird die existierende Funktionalität einer Software verändert oder erweitert.. 117

**AJAX** **Asynchronous JavaScript and XML** ist ein Konzept für die asynchrone Datenübertragung zwischen Client und Server und wird meist zur schnellen Aktualisierung bestimmter Teile von Internetseiten verwendet.. 112

**AVI** **Audio Video Interleave (AVI)** ist ein verbreitetes Containerformat von Microsoft zum Speichern von Video- und Audio-Inhalten.. 143, 144

**BDSG** Das **Bundesdatenschutzgesetz (BDSG)** regelt die Belange der Speicherung und des Zugriffs auf personenbezogene und -beziehbare Daten.. 48

**BIT** Bundesstelle für Informationstechnik im Bundesverwaltungsamt. 137

**BSI** Das **Bundesamt für Sicherheit in der Informationstechnik** ist der zentrale IT-Sicherheitsdienstleister des Bundes.. 48, 49, 112, 153, 154

**CI** **Codierte Informationen (CI)** sind Informationen, die in digitaler Form vorliegen und der Inhalt weiter verarbeitet werden kann.. 149

**CIFS** Das **Common Internet File System (CIFS)** ist ein von Microsoft ursprünglich unter dem Namen SMB entwickeltes Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Netzwerken. Die EU-Kommission verfügte 2004 dessen Offenlegung, was 2007 vom EUGH bestätigt wurde. Das OSS-Projekt SAMBA stellt eine freie Implementierung des Protokolls zur Verfügung.. 61, 62, 73, 74, 153

**Copyleft** Als **Copyleft** wird die zwingende Übertragung der Lizenz einer Software auf davon abgeleitete (geänderte, erweiterte, kombinierte) Werke, Wiederveröffentlichungen und Weitergaben der Software bezeichnet. Die bekannteste Copyleft-Lizenz ist die GPL, die dieses Prinzip begründete.. 18, 19, 31

**CSP** Die **Content Security Policy** ist ein Sicherheitskonzept des Webbrowsers Mozilla Firefox. Mit CSP können Web-Administratoren dem Browser durch Senden eines speziellen Headers (X-Content-Security-Policy: allow 'self';) mitteilen, welche Domains er als Quelle vertrauenswürdigen Codes akzeptieren soll.. 117

**CUPS** Das **Common Unix Printing System (CUPS)** kann beliebige Drucker über verschiedene Schnittstellen (Backends, z.B. IPP) ansprechen und über eine gemeinsame Schnittstelle im Netzwerk bereitstellen.. 61

**CVE** Die **Common Vulnerabilities and Exposures** sind ein Industriestandard, der Namenskonventionen für Sicherheitslücken und andere Schwachstellen definiert.. 51, 112, 113

**Desktop-Datenbank** Eine **Desktop-Datenbank** kombiniert die Datenverwaltung und Benutzeroberflächen zum Arbeiten mit den Daten in einem Programm.. 130

**DHCP** Das **Dynamic Host Control Protocol (DHCP)** dient der Zuweisung der Netzwerkkonfiguration an sich daran anmeldende Ressourcen und ist in RFC 2131 definiert.. 60

**DLZ-IT** Im März 2010 wurden das Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT), das Dienstleistungszentrum Informationstechnik im Geschäftsbereich des BMVBS (DLZ-IT BMVBS) sowie die Bundesstelle für Informationstechnik (BIT) vom IT-Rat zu **IT-Dienstleistungszentren des Bundes** ernannt. http://www.cio.bund.de/DE/IT-Angebot/IT-Dienstleistungszentren/dienstleistungszentren_node.html. 2, 28, 41, 90, 103, 172

**DMS** **Dokumentenmanagementsysteme (DMS)** sind Anwendungssysteme, die den vollen Lebenszyklus eines Dokuments verwalten. Dokumente repräsentieren im Kontext dieser System entweder NCI oder CI.. 149

**DMTF** Die **Distributed Management Tast Force (DMTF)** ist eine Normungsorganisation von Unternehmen der IT-Industrie zur Koordinierung von Entwicklung, Anpassung und Interoperabilität von Standards für das Systemmanagement.). 65, 87, 92

**DNS** Das **Domain Name System (DNS)** dient zum Übersetzen von Namen in numerische IP-Adressen und umgekehrt.. 60, 61, 73

**DOC** Das **Microsoft Office Word Binärformat** ist ein Microsoft Binärformat zum Speichern von Textverarbeitungs-Dokumenten.. 138, 139, 145

**DOCX** **Office Open XML Text** ist Teil des OOXML-Standards und dient zum Speichern von Textverarbeitungs-Dokumenten.. 139

**EUPL** Die **European Union Public Licence** ist eine Lizenz für Open-Source-Software mit strengem Copyleft-Effekt.. 133

**Extension** Skript-gesteuerte Erweiterung eines Browsers zur Änderung seines Aussehens oder Verhaltens. 113, 117

**FSFE** Die **Free Software Foundation Europe (FSFE)** ist nach eigener Aussage „eine gemeinnützige Organisation, die sich der Förderung Freier Software und der Arbeit für Freiheit in einer sich entwickelnden digitalen Gesellschaft widmet“.. 9, 167

**GIF** Grafikformat mit verlustfreier Komprimierung für Bilder mit geringer Farbtiefe und für kleine Animationen. 137, 138, 143, 144

**GPL** Die **GNU General Public License (GPL)** ist die bekannteste und am weitesten verbreitete Open-Source-Lizenz und enthält die Definition des sogenannten Copyleft. http://www.gnu.org/licenses/gpl.html. 18

**HDD** Das Dateiformat **Virtual Hard Disk Drive (HDD)** wurde von der Firma Parallels zur Bereitstellung virtueller Festplatten über die hauseigenen Produkte wie Parallels Desktop spezifiziert. Alternative Formate sind u.a. VMDK, QCOW und VHD.. 99, 100

**HTML** Die **Hypertext Markup Language** ist eine Auszeichnungssprache zur Darstellung und Verknüpfung von Inhalten in Internetseiten.. 123, 143

**HTTP** Das **Hypertext Transfer Protocol** ist ein Netzwerk-Protokoll, primär geschaffen zur Übertragung von HTML-Dateien, also von Internetseiten, wird aber aufgrund seines generischen Aufruf-Konzepts auch für diverse andere Zwecke verwendet.. 12

**IEEE** Das **Institute of Electrical and Electronics Engineers (IEEE)** ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik, der u.a. bei der Standardisierung von Techniken, Hardware und Software mitwirkt.). 88, 171

**IETF** Die **Internet Engineering Task Force (IETF)** ist eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst. Sie verwaltet u.a. die sogenannten Requests for Comments (RfC), in denen die Standards und Protokolle des Internet dokumentiert sind.. 60, 71

**IP** Das **Internet Protocol (IP)** ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es ist die Implementierung der Internetschicht des TCP/IP-Modells und der Vermittlungsschicht (engl. Network Layer) des OSI-Modells und in den RFCs 791 (IPv4) sowie 2460 (IPv6) definiert.. 60

**IPP** Das **Internet Printing Protocol (IPP)** stellt Druckdienste über ein Netzwerk auf der Basis von HTTP zur Verfügung.. 61

**ISO** Die **International Organization for Standardization (ISO)** entwickelt und veröffentlicht internationale Standards im privatwirtschaftlichen und öffentlichen Sektor. Sie setzt sich aus Vertretern nationaler Normungsgremien von derzeit 162 Staaten zusammen und hat ein Generalsekretariat mit Sitz in Genf.. 163

**ITIL** Die **IT Infrastructure Library (ITIL)** ist eine Sammlung von Best Practices in einer Reihe von Publikationen, die eine mögliche Umsetzung eines IT-Service-Management (ITSM) beschreiben und inzwischen international als De-facto-Standard hierfür gelten. In dem Regel- und Definitionswerk werden die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, die Aufbauorganisation und die Werkzeuge beschrieben. http://www.itil-officialsite.com/home/home.aspx. 38

**JPEG** Grafikformat der Joint Photographic Experts Group, meist in Verbindung mit verlustbehafeteter Komprimierung verwendet. 137, 138, 143, 144, 153

**KVM** Die **Kernel-based Virtual Machine (KVM)** ist eine freie Erweiterung des Linux-Kernels, der diesen zu einem vollwertigen Hypervisor ausbaut und gängige Hardware-Virtualisierungstechniken wie Intel-VT und AMD-V unterstützt.. 88, 93

**LDAP** Das **Lightweight Directory Access Protocol (LDAP)** dient dem gegenüber dem X.500-Standard vereinfachten Zugriff auf Verzeichnisdienste.. 12, 14, 15, 71, 73, 93, 97, 106, 153

**LPDP** Zum **Line Printer Daemon Protocol (LPDP)** ist ein ursprünglich für UNIX entwickeltes System, um Druckaufträge im Netzwerk verschicken zu können.. 61

**Microsoft Binärformat** Das **Microsoft Binärformat** ist ein für Menschen nicht unmittelbar lesbares Format zum Speichern von Office-Dokumenten als Binärdateien und war bis Microsoft Office 2003 das Standard-Dokumentenformat für dessen Komponenten.. 153

**MOV** **Quicktime Movie (MOV)** ist ein verbreitetes Containerformat von Apple zum Speichern von Video- und Audio-Inhalten in verschiedenen Formaten und die Basis von MP4.. 143, 144

**MP4** **MPEG-4 Part 14 (MP4)** ist ein unter ISO/IEC 14496-14 standardisiertes Containerformat zum Speichern von Video- und Audio-Inhalten in verschiedenen Formaten.. 143, 144

**MPEG-2** Der **Motion Picture Experts Group Standard 2** ist ein generischer MPEG-Standard zur Videokodierung mit Videokompression und Audiokodierung mit Audiokompression.. 143

**NCI** **Nicht-codierte Informationen (NCI)** sind Informationen, die entweder in Papierform vorliegen oder durch Scannen digitalisiert werden.. 149

**OCR** Die **Optical Character Recognition (OCR)** ist ein Verfahren zum Erkennen und Auslesen schriftlicher Informationen aus Bilddaten.. 165, 166

**ODF** Das **OASIS Open Document Format for Office Applications (ODF)** ist ein international genormter, quelloffener Standard für Dateiformate von Bürodokumenten (Textverarbeitung, Tabellenkalkulation, Präsentationen, Zeichnungen und Diagramme) auf der Basis der Extensible Markup Language (XML) und wurde 2006 als internationale Norm ISO/IEC 26300 veröffentlicht.. 129, 133, 136, 145

**ODMA** „Innerhalb der AIIM (Association for Information and Image Management) ist die ODMA-Gruppe (Open Document Management API) als Standardisierungsgremium tätig. ODMA bezeichnet eine standardisierte Schnittstelle zwischen dem Dokumentenmanagementsystem und den Benutzeranwendungen. Es vereinfacht an dieser Stelle die Einbindung der Anwendungen. Die meisten Anbieter unterstützen diesen Standard.[5], abgerufen: 12.08.2011“. 152

**ODP** **OpenDocument Presentation** ist Teil des ODF-Standards und dient zum Speichern von Präsentations-Dokumenten.. 143

**ODS** **OpenDocument Spreadsheet** ist Teil des ODF-Standards und dient zum Speichern von Tabellenkalkulations-Dokumenten.. 137, 141

**ODT** **OpenDocument Text** ist Teil des ODF-Standards und dient zum Speichern von Textverarbeitungs-Dokumenten.. 138

**OOXML** Die **Office Open XML File Formats (OOXML)** sind ein von Microsoft auf der Basis von Microsoft Office 2008 entwickelter offener Standard für XML-basierte Dateiformate zur Speicherung von Bürodokumenten(Textverarbeitung, Tabellenkalkulation, Präsentationen, Zeichnungen und Diagramme) und wurden 2008 als internationale Norm ISO/IEC 29500 veröffentlicht.. 134, 136, 145

**OSGi** Die **OSGi Service Platform (OSGi)** spezifiziert eine offene, einheitliche und vollständig modulare Architektur für die Entwicklung, Bereitstellung und Verwaltung von Diensten auf der Basis der Java Virtual Machine.. 15

**OSI** Die **Open Source Initiative (OSI)** ist eine gemeinnützige Organisation zur Förderung von OSS. Sie zertifiziert Open-Source-Lizenzen anhand einer von ihr selbst aufgestellten Definition von Open Source.. 17

**OSS** Mit **Open-Source-Software (OSS)** wird jede Software bezeichnet, die unter einer von der OSI anerkannten Open-Source-Lizenz steht.. 15, 77

**OVF** Das **Open Virtualization Format (OVF)** ist ein offener Standard für das Verpacken und Bereitstellen einer oder mehrerer virtueller Maschinen. Virtuelle Festplatten werden dabei gemeinsam mit Meta-Informationen zu den virtuellen Maschinen (z.B. Anzahl CPUs) verpackt. Der Standard wurde von der DMTF entwickelt und vom ANSI unter dem Bezeichner INCITS 469-2010 ratifiziert.). 87, 92, 93

[5] https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02259.html

**PDF** Das **Portable Document Format (PDF)** ist ein Dateiformat zur originalgetreuen Weitergabe von Dokumenten unabhängig von Anwendungsprogramm, Betriebssystem oder Hardware-Plattform und wurde 2008 als ISO 32000-1:2008 (PDF 1.7) veröffentlicht.. 133, 143, 145, 163

**PDF/A** Das **Portable Document Format zur Langzeitarchivierung (PDF/A)** ist ein Dateiformat zur originalgetreuen Langzeitarchivierung von Dokumenten basierend auf PDF 1.4 und wurde 2005 als internationale Norm ISO 19005-1:2005 veröffentlicht.. 146, 153

**Plug-In** Binäre Erweiterung eines Browsers mit unmittelbarem Zugriff auf Betriebssystem-Ressourcen zur performanten Darstellung eines bestimmten Medientyps. 113, 117

**PNG** Grafikformat für Rastergrafiken mit verlustfreier Bildkompression. 137, 138, 143, 144

**PPT** Das **Microsoft Office Powerpoint Binärformat** ist ein Microsoft Binärformat zum Speichern von Präsentations-Dokumenten.. 143, 144

**PPTX** **Office Open XML Presentation** ist Teil des OOXML-Standards und dient zum Speichern von Präsentations-Dokumenten.. 143

**PUE** Die **Power Usage Effectiveness (PUE)** ist das Maß der zusätzlich zum eigentlichen Nutzstrom für IT-Komponenten erforderlichen Energie für Klimatisierung, Notstromversorgung und andere Infrastrukturkomponenten des Rechenzentrumsbetriebes.. 40

**QCOW** Das Dateiformat **QEMU Copy On Write (QCOW)** wurde vom freien Emulator QEMU zur Bereitstellung virtueller Festplatten spezifiziert und liegt inzwischen als QCOW2 vor. Die Spezifikation steht unter http://sourceforge.net/projects/libqcow/files/Documentation/QEMU%20Copy-On-Write%20file%20format.pdf/download zur Verfügung. Alternative Formate sind u.a. VMDK, VDI und VHD.. 86, 88

**RDP** Das **Remote Desktop Protocol (RDP)** ist ein proprietäres Netzwerkprotokoll von Microsoft zum Darstellen und Steuern von Desktops auf fernen Computern.. 87

**RFB** Das **Remote Framebuffer Protocol (RFB)** ist ein freies Netzwerkprotokoll zum Darstellen und Steuern ferner grafischer Benutzerschnittstellen auf der Pixel-Ebene (Frame buffer) und durch diese Zugriffsart prinzipiell Plattform-unabhängig. Das RFB wird vom VNC implementiert.). 87

**RHEL** **Red Hat Enterprise Linux (RHEL)** ist eine der führenden Linux-Distributionen im Unternehmens-Umfeld.). 107

**RIA** Realisierung der Funktionalität eines Rich-Clients im Webbrowser. 112

**RTF** Das **Rich Text Format** ist ein von Microsoft 1987 eingeführtes plattformunabhängiges Format zum Datenaustausch zwischen Textverarbeitungsprogrammen verschiedener Hersteller.. 138, 139, 145

**SLA** Mit einem **Service Level Agreement (SLA)** werden gemäß ITIL bestimmte Betriebs-Dienstleistungen zu einem Produkt vereinbart, beispielsweise dessen Verfügbarkeit oder Reaktionszeiten bei Störungen.. 17, 38

**SLES** **Suse Linux Enterprise Server (SLES)** ist eine der führenden Linux-Distributionen im Unternehmens-Umfeld.). 107

**SMB** Zum **Server Message Block Protokoll (SMB)** siehe CIFS.. 61, 74

**SOA** Die **Service-orientierte Architektur (SOA)** ist ein Paradigma der Software-Architektur, das die Bereitstellung, Verknüpfung und Verwaltung modularer dynamischer Einheiten (Dienste) umfasst.. 13

**SPICE** Das **Simple Protocol for Independent Computing Environments (SPICE)** ist ein offenes Protokoll zum Darstellen und Steuern von Desktops auf fernen Computern. Es definiert die Bestandteile SPICE Driver (Gasterweiterung), Device (Wirts-Erweiterung) und Client (Zugriffssoftware) und zeichnet sich durch einen selbstoptimierenden Umgang mit Systemresourcen (Netzwerkbandbreite, für Desktop-Rendering verfügbare CPUs/GPUs auf Client und Server) aus. SPICE wurde von der inzwischen von Red Hat übernommenen Firma Qumranet entwickelt und 2009 unter OSS-Lizenzen freigegeben.. 87, 97

**SVG** XML-basiertes Grafikformat, vom W3C empfohlene Spezifikation zur Beschreibung zweidimensionaler Vektorgrafiken. 137, 138, 143, 144

**SWF** Abspielbare Adobe-Flash-Animationen. 143, 144

**SXI SUN XML Impress** ist ein XML-basiertes Format früherer Star-/OpenOffice-Versionen und dient zum Speichern von Präsentationen.. 143, 144

**SXW SUN XML Writer** ist ein XML-basiertes Format früherer Star-/OpenOffice-Versionen und dient zum Speichern von Textverarbeitungs-Dokumenten.. 138, 139

**TCP** Das **Transmission Control Protocol (TCP)** ist ein zuverlässiges, verbindungsorientiertes, paketvermittelndes Transportprotokoll in Computernetzwerken und ein Teil der Internetprotokollfamilie.. 60

**TIFF** Das **Tagged Image File Format (TIFF)** ist ein Dateiformat zur Speicherung von Bildern.. 153

**UML** Die **Unified Markup Language (UML)** ist ist eine graphische Modellierungssprache zur Spezifikation, Konstruktion und Dokumentation von Software-Teilen und anderer Systeme (Obj10). 158

**VDI** Das Dateiformat **Virtual Desktop Image (VDI)** wurde von der Innotek GmbH zur Bereitstellung virtueller Festplatten über die VirtualBox spezifiziert. Innotek und deren VirtualBox wurden 2008 von SUN übernommen, welche wiederum 2009 von Oracle gekauft wurde. VDI ist bis heute das Standardformat für virtuelle Maschinen der Oracle VirtualBox. Alternative Formate sind u.a. VMDK, QCOW und VHD.. 86, 88, 99

**VHD** Das Dateiformat **Virtual Hard Disk (VHD)** wurde von Connectix zur Bereitstellung virtueller Festplatten über das Produkt Virtual PC spezifiziert. Connectix und deren Virtual PC wurden 2003 von Microsoft gekauft. VHD dient heute als Standardformat für die Virtualisierungslösungen von Microsoft und Citrix (Xen). Die Spezifikation steht unter http://www.microsoft.com/openspecifications/en/us/programs/osp/virtualization-specifications/default.aspx zur Verfügung. Alternative Formate sind u.a. VDI, QCOW und VMDK.. 86, 88, 93, 99

**VMDK** Das Dateiformat **Virtual Machine Disk (VMDK)** wurde von VMware zur Bereitstellung virtueller Festplatten über die eigenen Virtualisierungsprodukte spezifiziert. Die Spezifikation steht unter http://www.vmware.com/technical-resources/interfaces/vmdk_access.html zur Verfügung. Alternative Formate sind u.a. VDI, QCOW und VHD.. 86, 88, 99

**VNC** Das **Virtual Network Computing (VNC)** ist eine Implementierung des RFB zum Darstellen und Steuern von Desktops auf fernen Computern. Es existieren verschiedene Derivate der ursprünglichen Entwicklung, u.a. RealVNC und TightVNC, mit unterschiedlichen zusätzlichen Fähigkeiten.). 87

**WCMS Ein Web-Content-Management-System (WCMS)** ist ein Fachverfahren, welches das Management des gesamten Lebenszyklus eines Web-Inhaltes unterstützt. Web-Inhalte im behördlichen Kontext sind alle Dateien, die zur Veröffentlichung im Internet tauglich sind und gleichzeitig von

SAGA (Die11b) erlaubt bzw. empfohlen werden. Die aus dem Lebenszyklus eines Web-Inhalts resultierenden Aufgaben sind folgende: Erstellen, Speichern, Kontrollieren/ Freigeben, Publizieren, Archivieren und Wiederfinden von Web-Inhalten. Bei diesen Aufgaben muss das WCMS den Anwender unterstützen.. 155, 158

**WebDAV Web-based Distributed Authoring (WebDAV)** and Versioning [...] is a set of extensions to the HTTP protocol which allows users to collaboratively edit and manage files on remote web servers.[6]“. 153

**WMV Windows Media Video** ist ein proprietärer Video-Codec von Microsoft und Teil der Windows-Media-Plattform.. 144

**WSDL** XML-basierte Beschreibungssprache für Web-Services. 152, 153

**XLSX Office Open XML Spreadsheet** ist Teil des OOXML-Standards und dient zum Speichern von Tabellenkalkulations-Dokumenten.. 142

**XML** Die Extensible Markup Language (engl. für „erweiterbare Auszeichnungssprache“) ist eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten in Form von Textdateien.. 153

**XSS Cross-Site-Scripting** ist eine Internet-basierte Angriffsart über Browser-Schwachstellen. 116

[6] http://webdav.org/, abgerufen: 18.08.2011